Løsningsforslag Øving 5
TMA4140-MA0302 Diskret matematikk
Høsten 2005

1.
a) Ingen andre tall enn en deler en, og en deler fire, så $(1, 4) = 1$
b) 1
c) 7 er et primtall og 7 er ikke en faktor i 41, så største felles divisor er 1. Vi kan også bruke Euklids algoritme:

$$\begin{aligned} 41 &= 7 \cdot 5 + 6 \\ 7 &= 6 + 1 \end{aligned}$$

d)

$$\begin{aligned} 42 &= 5 \cdot 8 + 2 \\ 5 &= 2 \cdot 2 + 1 \end{aligned}$$

Så største felles divisor er 1.
e)

$$\begin{aligned} 432 &= 21 \cdot 20 + 12 \\ 21 &= 12 + 9 \\ 12 &= 9 + 3 \\ 9 &= 3 \cdot 3 \end{aligned}$$

Så største felles divisor er 3.
f) La $d = (4321, 1234)$.

$$\begin{aligned} 4321 &= 1234 + 619 \text{ så } d|619 \\ 1234 &= 619 + 615 \text{ så } d|615 \\ 619 &= 615 + 4 \text{ så } d|4 \\ 615 &= 4 \cdot 153 + 3 \text{ så } d|3 \\ 4 &= 3 + 1 \text{ så } d|1 \end{aligned}$$

så største felles divisor er 1. (Vi kunne for eksempel stoppet i den tredje ligningen, siden hvis d ikke var en så måtte vi ha at 2 delte 615, noe som jo ikke er tilfellet.)

2.
I de tre første delene av denne oppgaven kan vi bruke arbeidet fra oppgave 1, henholdsvis del d, e og c.
a)

$$\begin{aligned} 1 &= 5 - 2 \cdot 2 \\ &= 5 - (42 - 5 \cdot 8) \cdot 2 = 17 \cdot 5 - 2 \cdot 42 \end{aligned}$$

Dermed kan vi ta $s = 17$ og $t = -2$.
b) $3 = 12 - 9 = 2 \cdot 12 - 21 = 2 \cdot 432 - 41 \cdot 21$. Dermed har vi
$6 = 4 \cdot 432 - 82 \cdot 21$, så vi kan ta $s = 4$ og $t = -82$.
c) Ved å regne som i oppgave a) får vi at $1 = 6 \cdot 7 - 41$. Ved å gange hver side med 8 får vi $8 = 48 \cdot 7 - 8 \cdot 41$. Dermed kan vi ta $s = 48$ og $t = -8$.
d) Vi bruker først Euklids algoritme for å finne $d = (123456, 654321)$ for å se om ligningen i det hele tatt har løsninger.

$$\begin{aligned} 654321 &= 123456 \cdot 5 + 37041 \\ 123456 &= 37041 \cdot 3 + 12333 \\ 37041 &= 12333 \cdot 3 + 42 \\ 12333 &= 42 \cdot 293 + 27 \\ 42 &= 27 + 15 \\ 27 &= 15 + 12 \\ 15 &= 12 + 3 \\ 12 &= 3 \cdot 4 \end{aligned}$$

så største felles divisor er 3, så det er mulig å løse ligningen. For å løse ligningen "går vi nå baklengs" gjennom utregningene over.

$$\begin{aligned} 3 &= 15 - 12 \\ &= 15 - (27 - 15) = 2 \cdot 15 - 27 \\ &= 2(42 - 27) - 27 = 2 \cdot 42 - 3 \cdot 27 \\ &= 2 \cdot 42 - 3(12333 - 42 \cdot 293) = 881 \cdot 42 - 3 \cdot 12333 \\ &= 881(37041 - 12333 \cdot 3) - 3 \cdot 12333 = 881 \cdot 37041 - 2646 \cdot 12333 \\ &= 881 \cdot 37041 - 2646(123456 - 37041 \cdot 3) = 8819 \cdot 37041 - 2646 \cdot 123456 \\ &= 8819(654321 - 123456 \cdot 5) - 2646 \cdot 123456 \\ &= 8819 \cdot 654321 - 46741 \cdot 123456 \end{aligned}$$

Dermed kan vi ta $s = -46741$ og $t = 8819$.

(Dette ble en del arbeid, men tallene var jo også store. Du kan overbevise deg om hvor effektiv denne metoden er ved å prøve følgende. For å sjekke

om vi i det hele tatt kan løse ligningen må vi finne største felles divisor. Den eneste alternative metoden vi kan for dette er primtallsfaktorisering. Du kan jo prøve det på disse tallene. Deretter, selv om vi nå vet at vi har en løsning, hvordan vil du finne den uten denne metoden??)

3.
Vi kan finne en løsning S og T som i oppgaven over. Denne fremgangsmåten gir $S = -2$ og $T = 5$. La nå s og t være en løsning (vi vet dette er oppfyllt for minst et par, nemlig $s = S$ og $t = T$). Da har vi

$$\begin{aligned} 42s + 17t &= 1 \\ 42S + 17T &= 1 \end{aligned}$$

Dette gir oss $42s + 17t = 42S + 17T$, som kan omskrives som $s - S = -\frac{17}{42}(t - T)$. Siden vi bare har med heltall å gjøre, og siden 17 og 42 er relativt primiske (m.a.o. de har ingen felles faktor) så ser vi at $t - T$ må være delelig med 42, m.a.o. det finnes et heltall k slik at $t - T = 42k$. Ved å gjøre tilsvarende arbeid finner vi at det finnes et heltall l slik at $s - S = 17l$. Setter vi disse to tingene inn i ligningene finner vi at vi må ha $l = -k$. Dermed er løsningene $s = -2 - 17l$ og $t = 5 + 42l$.

4.
29 er et primtall og 29 deler ikke 7. Dermed forteller Fermats lille setning oss at $7^{28} \equiv 1 \pmod{29}$. Siden $(7^{28})^3 = 7^{84}$ gir dette $7^{84} \equiv 1 \pmod{29}$, så $7^{89} \equiv 7^5 \pmod{29}$. M.a.o. $7^{89} \bmod 29 = 7^5 \bmod 29$. $7^5 = 16807$ og $16807 = 579 \cdot 29 + 16$. Dermed har vi $7^{89} \bmod 29 = 16$.

Alternativ løsning:
Vi bruker algoritme 5, s. 176 i boken. Vi bruker samme notasjon som i boken, og starter med $x = 1$ og $power = 7 \bmod 29 = 7$. Siden $89 = (1011001)_2$ har vi:
$i = 0:$ $a_0 = 1$, så $x = 1 \cdot 7 \bmod 29 = 7$ og $power = 7^2 \bmod 29 = 20$;
$i = 1:$ $a_1 = 0$, så $x = 7$ og $power = 20^2 \bmod 29 = 23$;
$i = 2:$ $a_2 = 0$, så $x = 7$ og $power = 23^2 \bmod 29 = 7$;
$i = 3:$ $a_0 = 1$, så $x = 7 \cdot 7 \bmod 29 = 20$ og $power = 7^2 \bmod 29 = 20$;
$i = 4:$ $a_0 = 1$, så $x = 20 \cdot 20 \bmod 29 = 23$ og $power = 20^2 \bmod 29 = 23$;
$i = 5:$ $a_0 = 0$, så $x = 23$ og $power = 23^2 \bmod 29 = 7$;
$i = 6:$ $a_0 = 1$, så $x = 23 \cdot 7 \bmod 29 = 16$.
Dermed er $7^{89} \bmod 29 = 16$.

5.

a) Euklids algoritme gir

$$\begin{aligned} 23 &= 19+4 & \qquad 1 &= 4-3 \\ 19 &= 4\cdot 4+3 & &= 4-(19-4\cdot 4) = 5\cdot 4-19 \\ 4 &= 3+1 & &= 5(23-19)-19 = 5\cdot 23-6\cdot 19. \end{aligned}$$

Fra dette ser vi at -6 er en invers til 19 modulo 23.
b) 38 er ikke relativt primisk 19 (det er faktisk et multiplum av 19), så det er ikke mulig å finne en slik invers.
c) I oppgave 2 så vi at 123456 og 654321 ikke er relativt primiske, så det finnes ingen slik invers.
d) Går vi "baklengs" gjennom utregningene i 1.d) får vi $1 = 17\cdot 5 - 2\cdot 42$. Vi ser fra dette at 17 er en invers til 5 modulo 42.
e) 42 er kongruent med 2 modulo 5, derfor finner vi heller en invers til 2 modulo 5. Vi ser at 3 er en slik invers siden 2 ganger 3 er 6, som igjen er kongruent med 1 modulo 5.

6.
a) Vi ser lett at vi kan ta $x = 2$. Vi kan evt. bruke metodene under
b) La oss starte med å finne en invers til 2 modulo 11. Vi ser at 6 er en slik invers siden 6 ganger 2 er 12 som er kongruent med 1 modulo 11. Hvis vi ganger dette med 5 får vi at 2 ganger 6 ganger 5 er kongruent med 5 modulo 11. Vi kan med andre ord ta $x = 5\cdot 6 = 30$ evt. $x = 8$ siden 8 og 30 er kongruente modulo 11.
c) Vi starter med å bytte ut 14 med 3, siden disse er kongruente modulo 11. Dermed ser vi lett at $x = 1$ gir en løsning.

7.
Vi starter med å observere at 14 er kongruent med 7 modulo 7. Altså må vi finne løsninger til ligningen $27x \equiv 0 \pmod 7$. Dette betyr at $27x$ må være et multiplum av 7. Siden 7 er et primtall og ikke er en faktor i 27 følger det at dette skjer hvis og bare hvis x er et multiplum av 7, m.a.o. $x = 7k$, k heltall, er alle løsningene.

8.
a) Vi starter med å finne en invers, y_1, til 78 modulo 7. Vi kan f.eks. ta $y_1 = 1$ (hvorfor?). Deretter setter vi $x_1 = 3\cdot 78\cdot 1$. Dette gir et tall som "passer i den første ligningen og som er null i den andre." Tilsvarende finner vi at -11 er en invers til 7 modulo 78, og at $x_2 = 2\cdot 7\cdot(-11)$ er "en løsning i den andre ligningen og null i den første." Dermed er $x = x_1 + x_2 = 234 - 154 = 80$ en løsning. Fra den kinesiske restsetningen får vi at $x = 80 + 546k$, k heltall, er alle løsningene (78 ganger 7 er 546.)

b) 2 er en invers til 396 modulo 7, 1 er en invers til 693 modulo 4, 5 er en invers til 308 modulo 9 og -1 er en invers til 252 modulo 11. Hvis vi dermed tar $x_1 = 3(2 \cdot 396) = 2376$ $x_2 = 2 \cdot 693 = 1386$ $x_3 = 2(5 \cdot 308) = 3080$ $x_4 = 5((-1) \cdot 252) = -1260$ så vil den første passe i den første ligningen og være null alle andre steder, den andre passer i den andre ligningen og er null alle andre steder, og så videre. Vi får en løsning $x = 5582$.

Fra den kinesiske restsetningen vet vi at denne løsningen er entydig modulo 2772, så vi får at $x = 38 + 2772k$, k heltall, er alle løsningene.
c) I stedet for 48 kan vi bruke 2 og i stedet for 45 kan vi bruke -1. Ligningene blir da

$$2x - 3y \equiv 1 \pmod{23} \quad (1)$$
$$3x - 1y \equiv 3 \pmod{23} \quad (2)$$

Trekk tre ganger den andre ligningen fra den første, og gang resultatet med -1 på hver side. Dette gir oss $7x \equiv 8 \pmod{23}$. Ved å finne en invers til 7 modulo 23 og gange med 8 får vi (10 er en slik invers) at vi kan ta $x = 80$ som igjen er kongruent med 11 modulo 23. 23 og 48 er relativt primiske, så $x = 11 + 23k$ vil være alle muligheter for x. Setter vi dette inn ser vi at vi får $3y \equiv 21 \pmod{23}$, så vi får at $y = 7 + 23l$.

4.4.8
Ved binomialteoremet er koeffisienten

$$\binom{17}{9} 3^8 2^9 = 24310 \cdot 6561 \cdot 512 = 81,662,929,920.$$

4.4.22
a)
Vi viser at begge sider av ligningen teller de samme objektene.

La X være en mengde med n elementer, og la A, B være disjunkte delmengder av X med henholdsvis $k, r-k$ elementer. Venstre side av ligningen gir oss antall måter vi kan velge ut disse delmengdene på, nemlig produktet av antall måter vi kan velge ut r elementer som skal være med i $A \cup B$ og antall måter man kan velge ut k elementer av disse som skal være med i A. Høyre siden gir oss også antall måter å velge ut delmengdene A, B på, nemlig produktet av antall måter vi kan velge ut k elementer til A og antall måter å velge ut $r-k$ elementer til B fra de gjenværende elementene i X.

b)

Venstre side kan skrives som

$$\binom{n}{r}\binom{r}{k} = \frac{n!}{r!(n-r)!} \cdot \frac{r!}{k!(r-k)!} = \frac{n!}{k!(n-r)!(r-k)!},$$

og høyre side kan skrives som

$$\binom{n}{k}\binom{n-k}{r-k} = \frac{n!}{k!(n-k)!} \cdot \frac{(n-k)!}{(r-k)!(n-r)!} = \frac{n!}{k!(n-r)!(r-k)!}.$$

Så venstre og høyre side av ligningen er lik.