MA1301 TALLTEORI, HØST 2012
LØSNINGSSKISSE – MIDTSEMESTERPRØVE

Oppgave 1. For $n = 1$ får vi $1^2 = \binom{3}{3}$. Anta

$$1^2 + 3^2 + \ldots + (2k-1)^2 = \binom{2k+1}{3}$$

for en $k \geq 1$. Da har vi at

$$\begin{aligned}
1^2 + 3^5 + \ldots + (2k-1)^2 + (2k+1)^2 &= \binom{2k+1}{3} + (2k+1)^2 \\
&= \frac{(2k+1)!}{(2k-2)!3!} + (2k+1)^2 \\
&= \frac{(2k+1)!(2k)(2k-1)}{(2k)!3!} + \frac{3!(2k+1)!(2k+1)}{(2k)!3!} \\
&= \frac{(2k+1)!\left(4k^2 - 2k + 6(2k+1)\right)}{(2k)!3!} \\
&= \frac{(2k+1)!(4k^2 + 10k + 6)}{(2k)!3!} \\
&= \frac{(2k+1)!(2k+2)(2k+3)}{(2k)!3!} \\
&= \binom{2k+3}{3}
\end{aligned}$$

Oppgave 2. Vi bruker divisjonsalgoritmen til å finne $\gcd(119, 272)$.

$$\begin{aligned}
272 &= 2 \cdot 119 + 34 \\
119 &= 34 \cdot 3 + 17 \\
34 &= 17 \cdot 2 + 0
\end{aligned}$$

Regner vi oss bakover finner vi

$$17 = 119 - 34 \cdot 3 = 119 - (272 - 2 \cdot 119) \cdot 3 = -3 \cdot 272 + 7 \cdot 119.$$

Dette gir oss løsninger $x_0 = 7$ og $y_0 = -3$. Alle løsninger er da på formen

$$\begin{aligned}
x &= 7 + 16t \\
y &= -3 - 7t
\end{aligned}$$

for $t \in \mathbb{Z}$.

Oppgave 3. Ettersom $\gcd(3, 5) = 1$ og $\gcd(5, 7) = 1$ kan vi gange med inverser og skrive om likningssystemet til

$$\begin{aligned}
x &\equiv 2 \pmod{4} \\
x &\equiv 3 \pmod{5} \\
x &\equiv 3 \pmod{7}
\end{aligned}$$

Siden $\gcd(4, 5) = \gcd(4, 7) = \gcd(5, 7) = 1$ følger det fra det kinesiske restklasseteorem at likningssystemet har unik løsning modulo $4 \cdot 5 \cdot 7$. Vi benytter standard fremgangsmåte og får følgende kongruenslikninger

$$\begin{aligned}
35x_1 &\equiv 1 \pmod{4} \\
28x_2 &\equiv 1 \pmod{5} \\
20x_3 &\equiv 1 \pmod{7}
\end{aligned}$$

med løsninger $x_1 \equiv 3 \pmod{4}$, $x_2 \equiv 2 \pmod{5}$ og $x_3 \equiv -1 \pmod{7}$. Endelig løsning blir da

$$x \equiv 35 \cdot 3 \cdot 2 + 28 \cdot 2 \cdot 3 - 20 \cdot 3 \cdot 1 \equiv 38 \pmod{140}.$$

Date: 8. oktober 2012.

Oppgave 4. Vi bruker hintet og ser at $4444^{4444} \equiv (-2)^{4444} \pmod 9$. Videre er $(-2)^3 \equiv -8 \equiv 1 \pmod 9$. Dermed blir

$$4444^{4444} \equiv (-2)^{4444} \equiv (-2)^{1481\cdot 3+1} \equiv \left((-2)^3\right)^{1481} \cdot (-2) \equiv 1^{1481} \cdot (-2) \equiv -2 \equiv 7 \pmod 9.$$

Oppgave 5. Bruker hintet og benytter at hvis $\gcd(195, a) = 1$ så er $\gcd(3, a) = \gcd(5, a) = \gcd(13, a) = 1$. Fra Fermats teorem finner vi følgende:

$$\begin{aligned} a^{12} \equiv (a^2)^6 \equiv 1^6 \equiv 1 &\pmod 3 \\ a^{12} \equiv (a^4)^3 \equiv 1^3 \equiv 1 &\pmod 5 \\ a^{12} \equiv 1 &\pmod{13} \end{aligned}$$

Dette betyr at $3, 5, 13 | a^{12} - 1$ og fra korollar 2 til teorem 2.4 har vi at $3 \cdot 5 \cdot 13 | a^{12} - 1$ eller ekvivalent at $a^{12} \equiv 1 \pmod{3 \cdot 5 \cdot 13}$. Videre er $192 = 12 \cdot 16$ så $a^{192} \equiv 1 \pmod{195}$ og det følger at $a^{193} \equiv a \pmod{195}$. Vi må nå også vise at resultatet er sant for $a = 3, 5$ og 13. Fra argumentet over har vi at $3^{192} \equiv 1 \pmod{5 \cdot 13}$ eller $3^{192} - 1 = 5 \cdot 13 \cdot k$ for et heltall k. Multipliserer vi denne likningen med 3 finner vi at $3^{193} - 3 = 3 \cdot 5 \cdot 13 \cdot k$ som er ekvivalent med $3^{193} \equiv 3 \pmod{195}$. Resultatet følger fra tilsvarende argument for 5 og 13.