Steffen Haug

Øving 4

Diskret Matematikk

TMA4140

Oppgåver til seksjon 4.1

Oppgåve 6

Skal vise at gitt a, b, c, d heiltal, der $a \neq 0$, slik at $a|c$ og $b|d$, så må $ab|cd$. (*Må ikkje* $b \neq 0$ *òg?, står ikkje i oppgåva, men eg har antatt det*)

$$\left.\begin{array}{l} a \mid c \to \frac{c}{a} \in \mathbb{Z} \\ b \mid d \to \frac{d}{b} \in \mathbb{Z} \end{array}\right\} \to \frac{c}{a} \cdot \frac{d}{b} \in \mathbb{Z} \to ab \mid cd$$

Oppgåve 13d

Gitt a, b heiltal slik at $a \equiv 4 \pmod{13}$ og $b \equiv 9 \pmod{13}$ Skal finne heiltal c, $0 \leq c \leq 12$ slik at $c \equiv 2a + 3b \pmod{13}$

$$\begin{aligned} c &\equiv 2a + 3b && \pmod{13} \\ &\equiv 8 + 27 && \pmod{13} \\ &\equiv 35 && \pmod{13} \\ &\equiv 9 && \pmod{13} \end{aligned}$$

Oppgåve 38

Skal vise at n heiltal $\to n^2 \equiv 0$ eller $1 \pmod{4}$.

Bruker at $n^2 \ \mathbf{mod}\ 4 = (n \ \mathbf{mod}\ 4)^2 \ \mathbf{mod}\ 4$ (Korollar 2). Då held det å undersøkje $n \in \{0, 1, 2, 3\}$

n	n^2	$n^2 \pmod{4}$
0	0	0
1	1	1
2	4	0
3	9	1

Oppgåver til seksjon 4.2

Oppgåve 3b

$10\,0000\,0001_2 \to \text{Dec} = 512 + 1 = 513$

512	**256**	**128**	**64**	**32**	**16**	**8**	**4**	**2**	**1**
1	0	0	0	0	0	0	0	0	1

Oppgåve 7b

$80\text{E}_{16} \to \text{Bin} = 1000\,0000\,1110$

8	**0**	**E**
1000	0000	1110

Oppgåve 24a

$$1\text{AE}_{16} \times \text{BBC}_{16} = 13\text{B}5\text{C}8_{16}$$
$$1\text{AE}_{16} + \text{BBC}_{16} = \text{D}6\text{A}_{16}$$

Oppgåver sekskjon 4.3

Oppgåve 6

Antal nullar på slutten av 100! er so mange gongar talet kan delast på 10. Vi ser på primtalsfaktoriseringa av 100!, men ikkje direkte, fordi den er keisam å rekne ut.

Vi må finne ut kor mange gongar 5×2 opptrer i primtalsfaktoriseringa, og sidan 2 opptrer langt oftare enn 5 ser vi nærmare på 5. 5 opptrer som faktor i tala $5, 10, 15, 20, \cdots$, og av desse er det 20 i tala mellom 1 og 100. Tek vi hensyn til at 5 opptrer fire ekstra gongar for kvart tal der 25 er faktor (4 gongar) får vi at 5 opptrer 24 gongar i primtalsfaktoriseringa av 100!.

Alle som kan femgongen veit at 5 ikkje opptrer fleire gongar. Sidan 2 opptrer *minst* like mange gongar opptrer 5×2, altso 10, nøyaktig 24 gongar, og dermed veit vi at $\underline{\underline{\text{100! har 24 nullar på slutten}}}$.

Oppgåve 33

Implementerte eit program som utfører algoritma.

```python
def gcd(a, b):
    while b != 0:
        r = a % b
        a, b = b, r
    return a
```

c: gcd$(123, 277) \to 1$

d: gcd$(1529, 14039) \to 139$

Oppgåve 39e

gcd(213, 117) $\to 3$

$$
\begin{aligned}
213 &= 117 + 96 \\
117 &= 96 + 21 \\
96 &= 4 \times 21 + 12 \\
21 &= 12 + 9 \\
12 &= 9 + 3 \\
9 &= 3 \times 3
\end{aligned}
$$

Oppgåve 49

Kvart andre tal er deleleg på 2, og kvart tredje tal er deleleg på 3. I eit intervall på tre tal $n, n+1, n+2$ er der derfor alltid minst eitt tal som er deleleg på 2, og minst eitt som er deleleg på 3 (dette kan vera det same talet, til dømes 6 i $\{5, 6, 7\}$)

Sidan der er minst eitt som er deleleg på 2 og eitt som er deleleg på 3, er produktet av tala alltid deleleg på 6.

Oppgåver til seksjon 4.4

Oppgåve 5

b: Skal finne invsersen til 19 (mod 141)

Brukar Euclids algoritme:

$$\begin{aligned}141 &= 7 \times 19 + 8\\ 19 &= 2 \times 8 + 3\\ 8 &= 2 \times 3 + 2\\ 3 &= 2 + 1\end{aligned}$$

Uttrykkjer 1 som lineærkombinasjon av 141 og 19

$$\begin{aligned}1 &= 3 - 2\\ &= 3 - (8 - 2 \times 3)\\ &= -8 + 3 \times 3\\ &= -8 + 3(19 - 2 \times 8)\\ &= 3(19) - 7(8)\\ &= 3(19) - 7(141 - 19 \times 7)\\ &= 3(19) - 7(141) + 49(19)\\ &= 52(19) - 7(141)\end{aligned}$$

Altso har vi at 52 er inversen til 19 i mod 141.

`c:` Skal finne inversen til 55 (mod 89)

Bruker Euclids algoritme:

$$\begin{aligned}
89 &= 55 + 34 \\
55 &= 34 + 21 \\
34 &= 21 + 13 \\
21 &= 13 + 8 \\
13 &= 8 + 5 \\
8 &= 5 + 3 \\
5 &= 3 + 2 \\
3 &= 2 + 1
\end{aligned}$$

Uttrykkjer 1 som lineærkombinasjon av 55 og 89

$$\begin{aligned}
1 &= 3 - 2 \\
&= 3 - (5 - 3) \\
&= -5 + 2 \times 3 \\
&= -5 + 2(8 - 5) \\
&= 2 \times 8 - 3 \times 5 \\
&= 2 \times 8 - 3(13 - 8) \\
&= -3 \times 13 + 5 \times 8 \\
&= -3 \times 13 + 5(21 - 13) \\
&= 5 \times 21 - 8 \times 13 \\
&= 5 \times 21 - 8(34 - 21) \\
&= -8 \times 34 + 13 \times 21 \\
&= -8 \times 34 + 13(55 - 34) \\
&= 13 \times 55 - 21 \times 34 \\
&= 13 \times 55 - 21(89 - 55) \\
&= -21 \times 89 + 34 \times 55
\end{aligned}$$

Altso har vi at 34 er inversen til 55 i mod 89.

Oppgåve 8

Dersom `gcd(a, m)` > 1. Kan ein ikkje finne 1 uttrykt som lineærkombinasjon av a og m. Dette betyr at det ikkje finnast eit tal som multiplisert med a gir 1 i mod m.

Oppgåve 11a

Skal løyse kongruensen ved å bruke inversen funne i oppgåve 5. Multipliserer kongruensen med inversen for å isolere x.

$$\begin{aligned} 19x &\equiv 4 \pmod{141} \\ 52 \cdot 19x &\equiv 52 \cdot 4 \pmod{141} \\ x &\equiv 52 \cdot 4 \pmod{141} \rightarrow x \equiv 52 \cdot 4 \equiv 67 \pmod{141} \end{aligned}$$