Oppgave 1 – Diskrete logaritmer

1.1 Orden

Litt Python gjør livet enklere:

```python
[[(x**i) % 11 for i in range(1,11)] for x in range(1,11)]
```

α	α^2	α^3	α^4	α^5	α^6	α^7	α^8	α^9	α^{10}	Orden
1										1
2	4	8	5	10	9	7	3	6	1	**10**
3	9	5	4	1						5
4	5	9	3	1						5
5	3	4	9	1						5
6	3	7	9	10	5	8	4	2	1	**10**
7	5	2	3	10	4	6	9	8	1	**10**
8	9	6	4	10	3	2	5	7	1	**10**
9	4	3	5	1						5
10	1									2

Først satte jeg opp tabellen for $\mathbb{Z}_{12}$ – jeg etterlater den her for å hedre min innsats, om ikke annet:

α	α^2	α^3	α^4	α^5	α^6	α^7	Orden
1							1
2	4	8	4	8	4	…	-
3	9	3	9	3	…		-
4	4	4	4	…			-
5	1						2
6	0	0	…				
7	1						2
8	4	8	4	…			-

α	α^2	α^3	α^4	α^5	α^6	α^7	Orden
9	9	9	9	9	…		-
10	4	4	4	4	4	…	-
11	1						2

1.2 Diskrete logaritmer

Hver celle er en k slik at $\alpha^k = \beta$. De β-ene som er primitive elementer i $\mathbb{Z}_{12}$ er markert med fet skrift.

Bruker tabellen fra forrige oppgave og fyller inn:

α/β	1	**2**	3	4	5	**6**	**7**	**8**	9	10
2	10	1	8	2	4	9	7	3	6	5
3	5	X	1	4	3	X	X	X	2	X
4	5	X	2	1	2	X	X	X	3	X
5	5	X	2	3	1	X	X	X	4	X
6	10	9	2	8	6	1	3	7	4	5
7	10	3	4	6	2	7	1	9	8	5
8	10	7	6	4	8	3	9	1	2	5
9	10	X	3	2	4	X	X	X	1	X
10	2	X	X	X	X	X	X	X	X	1

Ser at en $k \in \{1, 3, 7, 9\}$ vil gi et primitivt element når et annet primitivt element opphøyes i den.

Oppgave 2 – Primitive elementer

2a)

Skal finne et primitivt element i $\mathbb{Z}_{41}$.

For å slippe å prøve meg fram *for* mye, prøvde jeg med litt Python-kode:

```python
prim_elem = lambda p: next(
        i for i in range(1,p) if (p-1) == min(
                j for j in range(1,p) if 1 == (i**j) % p))
```

Fant da **6**, som er det *minste* primitive elementet i $\mathbb{Z}_{41}$.

2b)

Vet at ordenen til ethvert element i en modulo-ring deler $p - 1$.

For et primitivt element α, er $\{\alpha^k \mid k \in \mathbb{Z}\}$ lik ringen elementet er primitivt i. De k-verdiene som gir primitive elementer, er α-logaritmene til de *andre* primitive elementene.

For $p = 11$ ser vi fra oppgave 1b at k-verdiene er 1, 3, 7 og 9, der 1 er den trivielle k-en som gir samme α tilbake. Alle disse er innbyrdes primiske med $p - 1 = 10$.

Det virker naturlig å anta at dette gjelder *generelt*.

Nei, jeg ser ikke hvordan dette kan vises generelt.

2c)

Fra forrige oppgave vet vi at ethvert primitivt element α opphøyd i en k som er innbyrdes primisk med $p - 1$, vil være et primitivt element. Det fins ingen flere slike k-er som gir primitive elementer. Ergo er antallet primitive elementer i $\mathbb{Z}_p^*$ lik antallet tall som er innbyrdes primisk med $p - 1$, som er gitt av Eulers totientfunksjon ϕ.

Altså må $\mathbb{Z}_p^*$ ha $\phi(p - 1)$ primitive elementer.

2d)

Med resultatet fra forrige oppgave, ser vi at $\mathbb{Z}_{41}$ har

$$\phi(p-1) = \phi(40) = \phi(2^3 \cdot 5) = 2^2(2-1)(5-1) = 4 \cdot 1 \cdot 4 = 16$$

primitive elementer.

Oppgave 3 – Shanks algoritme

Skrev en implementasjon av Shanks algoritme i Python:

```python
snd = lambda pair: pair[1] # Extracts second value in a tuple
m = floor(sqrt(n))
lhs = sorted((j, modpow(a, m*j, n)) for j in range(m),
    key=snd)
rhs = sorted((i, (b*inv(modpow(a, i, n), n)) % n) for i in range(m),
    key=snd)
j, i = next( # Raises StopIteration if no such pair exists
    (j, i) for ((j, y1), (i, y2)) in product(lhs, rhs) if y1 == y2)
return (m*j+i) % n
```

Fikk til svar at $\log_\alpha \beta \bmod p = \log_6 3 \bmod 41 =$ **15**.

Tester: $6^{15} \bmod 41 = 470184984576 \bmod 41 = 3$, som forventet.

Oppgave 4 – RSA-signering

I RSA har vi en privat nøkkel (p, q, d) og en offentlig nøkkel (n, e) slik at

$$n = pq$$

og

$$ed \equiv 1 \pmod{n}.$$

Dekrypteringsfunksjonen

$$d_K(x) = x^d \bmod n$$

kan brukes som signeringsfunksjon, og krypteringsfunksjonen

$$e_K(y) = y^e \bmod n$$

kan brukes til verifisering av en melding x – vi får signaturen (x, y).

Her er $(n, e) = (n, b) = (437, 13)$ og $(p, q, d) = (p, q, a) = (23, 19, 61)$.

4.1

Meldingene $(78, 394)$ og $(123, 289)$ skal verifiseres.

$$e_K(394) = 394^{13} \bmod 437 = 78$$
$$e_K(289) = 289^{13} \bmod 437 = 123.$$

Da er det sannsynlig at *begge* meldingene er sendt fra Bob.

4.2

Kan f.eks. la tallet $y = 42$ være signaturen. Da er

$$e_K(42) = 42^{13} \bmod 437 = 237$$

den originale meldingen, og den fulle meldingen er $(237, 42)$.

Riktignok vet vi ikke hva *innholdet* i denne meldingen er, men vi har nå et fullstendig legitimt forfalsket par av melding og signatur.

Dette skulle vel heller vært enveis?

4.3

…da endte jeg ikke opp med å gjøre denne. Skylder på at jeg er for trøtt akkurat nå, men det er ikke noen unnskyldning for omstendighetene som ledet meg hit.

4.4

Når meldingen skal signeres og krypteres, må signeringen gjøres *først*. Alice er avsender, så hennes kryptosystem utgjør basis for signeringen:

$n_A = 17 \cdot 43 = 731,\ e_A = 19,\ d_A = 283.$

$$\begin{aligned} x &= 109 \\ \underset{A}{\operatorname{sig}}(x) &= 109^{283} \bmod 731 = 31 \\ e_B(x, y) &= (109, 31)^{13} \bmod 437 = (401, 202) \end{aligned}$$

.

```
(109**283)%731
[(x**13)%437 for x in (109,31)]
```

Verifiserer ved å verifisere signeringen fra Bobs side. Han må dekyptere og så verifisere.

$$\begin{aligned} d_B(x_c, y_c) &= (401, 202)^{61} \bmod 437 = (109, 31) \\ e_A(x_d) &= 109^{19} \bmod 731 = 260 \\ &\Downarrow \\ \underset{A}{\operatorname{ver}}(x, y) &= \texttt{false}. \end{aligned}$$

Her har det åpenbart skjedd en eller annen feil. Jeg vet ikke hvor den ligger.

```
[(x**61)%437 for x in (401,202)]
(109**19)%731
```

Oppgave 5 – El Gamal-signering

5.1

Signeringssystemet basert på

$$\begin{gathered} 13^{15} \equiv 29 \pmod{37} \\ \Updownarrow \\ \log_{13} 29 \equiv 15 \pmod{37} \end{gathered}$$

har $K = (p, \alpha, a, \beta) = (37, 13, 15, 29)$

5.2

Med $k = 11$ blir $\operatorname{sig}_K(14, 11) = (\gamma, \delta) = (15, 13)$, der

$$\begin{aligned} \gamma &= \alpha^k \pmod{p} = 13^{11} \pmod{37} = 15 \\ \delta &= (x - \alpha\gamma) \cdot k^{-1} \pmod{p-1} = (14 - 13 \cdot 15) \cdot 23 \pmod{36} = 13. \end{aligned}$$

Verifiserer:

$$\begin{gathered} \beta^\gamma \gamma^\delta = 29^{15} 15^{13} \equiv 26 \pmod{37} \\ \alpha^x = 13^{14} \equiv 25 \pmod{37} \\ \Downarrow \\ \operatorname*{ver}_K(x, \gamma, \delta) = \texttt{false}. \end{gathered}$$

Med $k = 5$ blir $\operatorname{sig}_K(3, 5) = (\gamma, \delta) = (21, 18)$, der

$$\begin{aligned} \gamma &= \alpha^k \bmod p = 3^5 \bmod 37 = 21 \\ \delta &= (x - \alpha\gamma) \cdot k^{-1} \bmod p - 1 = (3 - 13 \cdot 21) \cdot 29 \bmod 36 = 18. \end{aligned}$$

Verifiserer:

$$\begin{aligned} \beta^{\gamma}\gamma^{\delta} = 29^{21}21^{18} &\equiv 31 \pmod{37} \\ \alpha^{x} = 13^{3} &\equiv 14 \pmod{37} \\ &\Downarrow \\ \underset{K}{\mathrm{ver}}(x, \gamma, \delta) &= \texttt{false}. \end{aligned}$$

Konklusjon: Jeg har gjort noe alvorlig galt her.

5.3

Verifiserer meldingen 32 med $(\gamma, \delta) = (19, 6)$:

$$\begin{aligned} \beta^{\gamma}\gamma^{\delta} = 29^{19}19^{6} &\equiv 14 \pmod{37} \\ \alpha^{x} = 13^{32} &\equiv 12 \pmod{37} \\ &\Downarrow \\ \underset{K}{\mathrm{ver}}(x, \gamma, \delta) &= \texttt{false}. \end{aligned}$$

Verifiserer meldingen 9 med $(\gamma, \delta) = (32, 16)$:

$$\begin{aligned} \beta^{\gamma}\gamma^{\delta} = 29^{32}32^{16} &\equiv 7 \pmod{37} \\ \alpha^{x} = 13^{9} &\equiv 6 \pmod{37} \\ &\Downarrow \\ \underset{K}{\mathrm{ver}}(x, \gamma, \delta) &= \texttt{false}. \end{aligned}$$

Konklusjon: Begge meldingene er falske *eller* jeg har gjort en grov feil. Sannsynligvis det siste.