Oppgave 1 - Moduloregning

$$232 + 22 \cdot 77 - 18^2 \pmod 8$$
$$\equiv 0 + 6 \cdot 5 - 2^2 \equiv 30 - 4 \equiv 6 - 4 \equiv 2 \pmod 8$$

Oppgave 2 - Gangetabell modulo 12

2a)

Begynte å gjøre det manuelt, skrev så et program for å gjøre det for meg.

·	1	2	3	4	5	6	7	8	9	10	11
1	**1**	2	3	4	5	6	7	8	9	10	11
2	2	4	6	8	10	0	2	4	6	8	10
3	3	6	9	0	3	6	9	0	3	6	9
4	4	8	0	4	8	0	4	8	0	4	8
5	5	10	3	8	**1**	6	11	4	9	2	7
6	6	0	6	0	6	0	6	0	6	0	6
7	7	2	9	4	11	6	**1**	8	3	10	5
8	8	4	0	8	4	0	8	4	0	8	4
9	9	6	3	0	9	6	3	0	9	6	3
10	10	8	6	4	2	0	10	8	6	4	2
11	11	10	9	8	7	6	5	4	3	2	**1**

2b)

Som vanlig 1 og 11, i tillegg 5 og 7. Alle har symmetriske multiplikative inverser.

2c)

Skal bevise følgende:

Ingen 0 eller 1 på samme rad/kolonne, dvs.: *Hvis a ikke har multiplikativ invers, fins en $b \not\equiv 0 \pmod{12}$ slik at $ab \equiv 0 \pmod{12}$*

Gitt et tall $a \in \mathbb{Z}_{12}$ slik at $\forall x \in \mathbb{Z}_{12},\ ax \not\equiv 1 \pmod{12}$

Om a hadde vært innbyrdes primisk med 12, hadde a hatt en multiplikativ invers modulo 12. Siden a *ikke* er innbyrdes primisk med 12, har 12 og a minst én felles faktor, og da vil det finnes et annet tall som består av de *andre* faktorene i 12 (og naturlig nok er mindre enn 12).

Hvorfor?
Trekker fram aritmetikkens fundamentalteorem. Et tall kan skrives som et produkt av primtall. 12 kan skrives $12 = 2^2 \cdot 3$. Når $\gcd(a, 12) > 1$, vil a være et produkt av en eller flere av faktorene til 12. La b være produktet av de gjenværende faktorene til 12 (siden $a < 12$ kan ikke a bestå av de samme faktorene som 12). Da er $ab =$ 1 eller flere av faktorene · de gjenværende faktorene $= 12k$, der k er et heltall, så $12|ab$ og $ab \equiv \pmod{12}$.

Altså: Da *må* det finnes et tall $b \in \mathbb{Z}_{12}$ som gir $ab \equiv 0 \pmod{12}$.

Dette kan skrives generelt for alle $\mathbb{Z}_N$

Oppgave 3 - Inverser

Invers matrise → kun hvis $\det A$ har multiplikativ invers i $\mathbb{Z}_n$

$$A = \begin{pmatrix} 2 & -1 \\ 5 & 8 \end{pmatrix}$$

3a)

Over $\mathbb{Z}_{10}$

$$\det A = 2 \cdot 8 - 5(-1) = 16 + 5 \equiv 6 + 5 = 11 \equiv 1 \pmod{10}$$

Siden $\det A \equiv 1$, som *har* en multiplikativ invers modulo 10 (seg selv), så har A har en invers modulo 10:

$$A^{-1} = \begin{pmatrix} 8 & 1 \\ -5 & 2 \end{pmatrix} \equiv \begin{pmatrix} 8 & 1 \\ 5 & 2 \end{pmatrix} \pmod{10}$$

Sløyfer $\frac{1}{\det A}$ foran, siden denne er lik 1.

3b)

Over $\mathbb{Z}_9$

$$\det A = 2 \cdot 8 - 5(-1) = 16 + 5 \equiv 7 + 5 = 12 \equiv 3 \pmod 9$$

3 har definitivt ikke en multiplikativ invers modulo 9, siden 3 og 9 ikke er innbyrdes primiske $(3|9)$, så A har **ikke** en invers over $\mathbb{Z}_9$.

Oppgave 4 - Substitusjonschifre

4a)

Antall nøkler avhenger av antallet tegn i alfabetet, fra kombinatorikken vet vi at antall permutasjoner der rekkefølgen har betydning, er

$$N! = 29! = 8,841761994 \cdot 10^{30}$$

4b)

Enkle grep Alice og Bob kan gjøre for å bedre sikkerheten:

- Gjøre nøkkelen lengre
- Involvere et annet konsept i chifferet

4c)

Blokker med n tegn, har en nøkkel som oversetter hver blokk ved å substituere med en av 29^n nøkler.

Altså: $(29^n)!$

Oppgave 5 - k-shift-chiffer

`YÆVFB VBVFR ÅVBV` er den krypterte meldinga.

Et k-shift-chiffer, men vi kjenner ikke k…

Skrev Haskell-kode for å dekryptere, fikk `HJERNENERALENE` …
Etter litt mistanke om feil i koden, kom jeg til at det skal tydes `HJERNEN ER ALENE` (igjen en sang) med $k = 17$.

Hvordan: Kjørte programmet, skrev den krypterte meldinga, fant da at det fornuftige var på linje 17 ved å pipe output til `nl` som setter linjenummer på tekst, og se etter `HJERNENERALENE`. Bekreftet dette ved å kjøre

```
map backlate $ decrypt (map translate "YÆVFBVBVFRÅVBV")29 17
```

som ga tilbake `HJERNENERALENE`. (ja, koden er litt rotete, beklager)

Bonus: I foilene var det en annen melding kryptert med k-shift-chiffer:
`WRTFVYURYYRBUNOVSS` → `JEGVILHELLERHABIFF`

Oppgave 6 - Blokkchiffer

Formell definisjon

Formell definisjon av et blokkchiffer basert på et k-shift-chiffer:

N tegn og blokkstørrelse b...

Kunne satt opp et chiffer mønster av Vigènere-chifferet, bare med én k som nøkkel:

$$\begin{aligned} \mathcal{P} = \mathcal{C} = (\mathbb{Z}_N)^b\,,\ \mathcal{K} = \{x \mid 0 \leq x < N\}, \\ e_k(x_1, x_2, \cdots, x_b) = (x_1 + k, x_2 + k, \cdots, x_b + k) \pmod N \\ d_k(x_1, x_2, \cdots, x_b) = (x_1 - k, x_2 - k, \cdots, x_b - k) \pmod N \end{aligned}$$

Men: Dette er ikke egentlig noe blokkchiffer siden k er en uniform nøkkel.

Siden Vigènere-chifferet bruker akkurat samme prinsipp som k-shift, bare med flere forskjellige k_i i nøkkelen $K = (k_1, k_2, \ldots, k_b)$, kan vi skrive

$$\begin{aligned} \mathcal{P} = \mathcal{C} = \mathcal{K} = \mathcal{K} = (\mathbb{Z})^b\,, \\ e_k(x_1, x_2, \cdots, x_b) = (x_1 + k_1, x_2 + k_2, \cdots, x_b + k_b) \pmod N \\ d_k(x_1, x_2, \cdots, x_b) = (x_1 - k_1, x_2 - k_2, \cdots, x_b - k_b) \pmod N \end{aligned}$$

som en *verdig* versjon av shift-chifre som blokkchiffer.

Antall forskjellige nøkler

Hver nøkkel i Vigènere-chifferet består av b like eller ulike tegn k_i, der $\forall k_i \in K,\ k_i \in \mathbb{Z}_N$, så chifferet har N^b ulike nøkler.

Oppgave 7 - Vigènere

7a)

Skal kryptere "Nå er det snart helg" med $K =$ "torsk".

Skrev litt Haskell-kode igjen og det årna sæ:

```
bl $ encryptNums 29 (tl "NÅERDETSNARTHELG") (tl "TORSK")
```

eller

```
encrypt "NÅERDETSNARTHELG" "TORSK"
```

Fikk `DNVGNXEGCKHEYWVZ` som den krypterte teksten, verifiserte at det gikk an å oversette tilbake.

(kjørte det bare i `ghci`-interpreteren, lagde ikke noen `main` for denne)

7b)

Skal dekryptere `QZQOBVCAFFKSDC` med nøkkelord `BRUS`

```
decrypt "QZQOBVCAFFKSDC" "BRUS"
```

Får `PIZZAELLERTACO` – ja takk, begge deler

7c)

m er antall tegn nøkkelen (og blokkene) består av. Med N tegn totalt, vil antall mulige nøkler være N^m (rekkefølgen har betydning, med tilbakelegging).

Eksempelvis for $N = 29$ tegn i alfabetet og en blokkstørrelse på $m = 4$:

$$N^m = 29^4 = 707281$$

Oppgave 8 - Hill

$$K = \begin{pmatrix} 11 & 8 \\ 3 & 7 \end{pmatrix}$$

8a)

Standard metode for invers av 2×2-matrise:

Først en test av determinanten:

$$\det K = 11 \cdot 7 - 3 \cdot 8 = 53 \equiv 24 \pmod{29}$$

Den er ikke lik 1, så vi får ikke en simpel $\frac{1}{1}$-brøk.
Vi må finne den multiplikative inverse til 24!

$$\begin{aligned}
29 &= 24 + 5 \\
24 &= 4 \cdot 5 + 4 \\
5 &= 4 + 1 \\
&\Downarrow \\
1 &= 5 - 4 \\
&= 5 - (24 - 4 \cdot 5) = -24 + 5 \cdot 5 \\
&= -24 + 5 \cdot (29 - 24) = 5 \cdot 29 - 6 \cdot 24 \\
&\Downarrow \\
1 &\equiv (-6) \cdot 24 \equiv 23 \cdot 24 \pmod{29}
\end{aligned}$$

Så: Den multiplikative inverse av 24 er 23 modulo 29.

Da får vi at den inverse av K er

$$\begin{aligned}
K^{-1} &= \frac{1}{\det K} \cdot \text{cof } K \\
&= \frac{1}{24} \cdot \text{cof} \begin{pmatrix} 11 & 8 \\ 3 & 7 \end{pmatrix} \equiv 23 \cdot \begin{pmatrix} 7 & -8 \\ -3 & 11 \end{pmatrix} \\
&\equiv \begin{pmatrix} 161 & -184 \\ -69 & 253 \end{pmatrix} \equiv \begin{pmatrix} 16 & 19 \\ 18 & 21 \end{pmatrix} \pmod{29}
\end{aligned}$$

8b)

Får kryptert `PRIM` til `NHID` ved å gange hver blokk i `PRIM` med K. Se hill.py, spesielt funksjonen `encpypt`, naturligvis.

8c)

Skal dekryptere meldingen `TOYYSN`. Skrev Python-kode for dekryptering, se spesifikt på funksjonen `decrypt_with_inv` der jeg gir den inverse fra 8a inn som parameter.

Resultat: `FREDAG`. Tatt i betraktning tendensen til å bruke fraser fra/titler på sangtekster i denne øvingen og i foilene, tror jeg det er ment som en del av "Men det er først på fredag". Det er først på fredag at øvinga har frist.

8d)

Vet at $m = 2$ og at "EASY" ble kryptert til "IØÅY".

Konverterte til tallverdier med Python-koden jeg skrev.

Skal altså finne en matrise K som tilfredsstiller

$$
\begin{aligned}
x_1K &= \begin{pmatrix} 4 & 0 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 8 & 27 \end{pmatrix} \pmod{29} \\
x_2K &= \begin{pmatrix} 18 & 24 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 28 & 24 \end{pmatrix} \pmod{29}
\end{aligned}
$$

Det gir systemene

$$
\begin{aligned}
\begin{pmatrix} 4a & 4b \end{pmatrix} &\equiv \begin{pmatrix} 8 & 27 \end{pmatrix} \pmod{29} \\
\begin{pmatrix} 18a + 24c & 18b + 24d \end{pmatrix} &\equiv \begin{pmatrix} 28 & 24 \end{pmatrix} \pmod{29} \\
&\Downarrow \\
a &= \frac{8}{4} = 2 \\
b &= \frac{27}{4} \equiv 27 \cdot 22 = 594 \equiv 14 \\
c &= \frac{28 - 18 \cdot 2}{24} = \frac{-8}{24} \equiv (-8) \cdot 23 = -184 \equiv 19 \\
d &= \frac{24 - 18 \cdot 14}{24} = \frac{-228}{24} \equiv 4 \cdot 23 = 92 \equiv 5
\end{aligned}
$$

(den multiplikative inverse til 4 er 22)

Vi ser da at

$$
K = \begin{pmatrix} 2 & 14 \\ 19 & 5 \end{pmatrix}
$$