Oppgave 1 (Gammel eksamensoppgave). Finn alle x i $\mathbb{Z}$ slik at
(a) $9x \equiv 7 \mod 12$.
(b) $6x \equiv 9 \mod 15$.

Fasit. (a) Vi har at $d = \gcd(9, 12) = 3$, mens $3 \nmid 7$. Dette medfører at denne likningen ikke er løsbar.

(b) Vi har at $d = \gcd(6, 15) = 3$ og at $d \mid 9$, slik at denne likningen er løsbar. Når vi faktoriserer/forkorter med d, får vi likningen

$$2x \equiv 3 \mod 5.$$

Inversen til 2 modulo 5 er 3, slik at $x = 3 \cdot 3 \equiv 4 \mod 5$. Alle heltallene z i $\mathbb{Z}$ som er kongruent modulo 5 til 4 er løsninger i den opprinnelige likningen, dvs.

$$4 + 5\mathbb{Z} = \{4 + m \cdot 5 \mid m \in \mathbb{Z}\}.$$

Oppgave 2. Vis følgende korollar av Setning 71.

Korollar 72. *La $n > 1$ være et kvadratfritt heltall, og la $a \in \mathbb{Z}$. For hver $k \geq 1$, så er*

$$a^{k\varphi(n)+1} \equiv a \mod n,$$

der φ betegner Eulers phi-funksjon.

Fasit. Vi viser dette ved induksjon på k.
$k = 1$: Dette er Setning 71.
$k > 1$: Anta sant for k, dvs. $a^{k\varphi(n)+1} \equiv a \mod n$. Vi har at

$$\begin{aligned} a^{(k+1)\varphi(n)+1} &= a^{\varphi(n)} a^{k\varphi(n)+1} \\ &\equiv a^{\varphi(n)} a \mod n, \text{ siden } a^{k\varphi(n)+1} \equiv a \mod n \\ &\equiv a^{\varphi(n)+1} \mod n \\ &\equiv a \mod n, \text{ av tilfellet } k = 1 \end{aligned}$$

Dette viser påstanden.

Oppgave 3, RSA. Alice ønsker å sende hemmelige meldinger til Bob. Alle kan lese hva som blir sendt, men likevel ikke klare å finne meldingen.

Vi har følgende antakelser: La p, q være to forskjellige primtall, og la $n = pq$. Da er $\varphi(n) = (p-1)(q-1)$. Velg e med $1 < e < \varphi(n)$ og $\gcd(e, \varphi(n)) = 1$, dvs. $\overline{e}$ har en inverse $\overline{d}$ i $\mathbb{Z}_{\varphi(n)}$ og $\overline{d} \cdot \overline{e} = \overline{1}$ i $\mathbb{Z}_{\varphi(n)}$ og $de - 1 = k\varphi(n)$ for en $k \geq 1$, der $1 < d < \varphi(n)$.

Alice: Hemmelig nøkkel $\{n, d\}$, og offentlig nøkkel $\{n, e\}$.

Bob: Vil sende en melding M, der $0 \leq M < n$, til Alice. Krypterer meldingen:

(i) Beregner N slik at $M^e \equiv N \mod n$, der $0 \leq N < n$.

(ii) Sender N til Alice.

Alice: (i) Mottar N.

(ii) Beregner $D(N)$ med $0 \leq D(N) < n$ slik at

$$N^d \equiv D(N) \mod n.$$

(a) Får Alice tilbake M? Er $M = D(N)$?

(b) Hva avgjør om dette gir en rimelig sikker/hemmelig måte å kommunisere på?

Fasit. (a) Vi har at

$$\begin{aligned} N^d &\equiv M^{de} \mod n, \text{ fra det over er: } de - 1 = k\varphi(n) \text{ for en } k \geq 1. \\ &\equiv M^{k\varphi(n)+1} \mod n \\ &\equiv M \mod n, \text{ fra Korollar 72.} \end{aligned}$$

Både M og $D(N)$ ligger mellom 0 og $n-1$, så er eneste måten vi kan ha $M \equiv D(N) \mod n$, er at $M = D(N)$.

(b) For $n = pq$ stor, hvor p og q er primtall, tar det lang tid å finne p og q. Vi trenger p og q til å finne $\varphi(n)$, som igjen er nødvendig for å dekryptere.