Oppgave 1 Finn alle løsninger av den diofantiske ligningen $72x + 177y = 6$.

Oppgave 2 Finn alle løsninger av systemet

$$\begin{aligned} x &\equiv 3 \pmod 6 \\ x &\equiv -4 \pmod 7 \\ x &\equiv 2 \pmod{11} \end{aligned}$$

Oppgave 3

a) Hva får vi til rest når vi deler 1301^{2023} på 33?

b) Hva får vi til rest når vi deler $2023 \cdot (1299!)$ på (primtallet) 1301?

Oppgave 4 I et RSA-kryptosystem er den offentlige krypteringsnøkkelen $\{n, e\}$ gitt ved $n = 221 = 13 \cdot 17$ og $e = 169$.

a) Finn den hemmelige dekrypteringseksponenten d.

b) Dekrypter $c = 6$.

Oppgave 5 Vis ved induksjon at

$$1^3 + 2^3 + \cdots + n^3 = \frac{n^2(n+1)^2}{4}$$

for alle $n \geq 1$.

Oppgave 6

a) Finn de primitive røttene til 11. Verifiser at 8 ikke har noen primitive røtter.

b) La p være et primtall og $n = 4p$. Vis at n ikke har noen primitive røtter.
Hint: vis at dersom p er odde og $\gcd(a, n) = 1$, så vil $a^{p-1} \equiv 1 \pmod n$.

Oppgave 7 La p være et odde primtall slik at $q = 4p+1$ også er et primtall (for eksempel $p = 3, q = 13$ eller $p = 7, q = 29$). Vis at den kvadratiske kongruensen

$$x^2 \equiv p \pmod q$$

er løsbar.