Exercise 1 (4 Punkte):
Let $\mathbb{F}_p$ be a finite field and let $N | p - 1$. Prove that $\mathbb{F}_p^*$ has an element of order $N$. This is true in particular for any prime power that divides $p - 1$. (Hint. Use the fact the $\mathbb{F}_p^*$ has a primitive root).

Exercise 2 (10 Punkte):
Using the Pohlig-Hellmann method, solve the dlog problem $\beta = \alpha^x \mod p$ for $(\alpha, \beta, p) = (2, 39183497, 41022299)$.

Provide all the intermediate steps of the algorithm: show the vector $(a_1, \ldots, a_k)$ that you use as an input to the CRT to determine $x$. Also, provide the values for $\alpha_i = \alpha^{\frac{p-1}{p_i e_i}}$ and $\beta_i = \beta^{\frac{p-1}{p_i e_i}}$, where $p - 1 = \prod_i p_i^{e_i}$.

Exercise 3 (4 Punkte):
If $f, g \in k[x]$, then prove that $\langle f - qg, g \rangle = \langle f, g \rangle$ for any $q \in k[x]$.

Exercise 4 (6 Punkte):

1. Compute GCD($x^3 + x^2 - 4x - 4, x^3 - x^2 - 4x + 4, x^3 - 2x^2 - x + 2$).

2. Decide whether $x^2 - 4 \in \langle x^3 + x^2 - 4x - 4, x^3 - x^2 - 4x + 4, x^3 - 2x^2 - x + 2 \rangle$