Problem 1. Let $f$ be an arbitrary function from $\mathbb{N}$ to $\mathbb{R}_{>0}$.

1. Let $g_1, g_2$ be two functions from $\mathbb{N}$ to $\mathbb{R}_{>0}$ such that $g_1$ and $g_2$ are both $\Theta(f)$. Show that the function $g_1 + g_2$ is $\Theta(f)$ or provide a counterexample.

2. With $g_1, g_2$ as above, show that the function $g_1g_2$ is $\Theta(f^2)$ or provide a counterexample.

3. Let $g_3, g_4$ be two functions from $\mathbb{N}$ to $\mathbb{R}$ such that $g_3$ and $g_4$ are both $\Theta(f)$. Show that the function $g_3 + g_4$ is $\Theta(f)$ or provide a counterexample.

4. With $g_3, g_4$ as above, show that the function $g_3g_4$ is $\Theta(f^2)$ or provide a counterexample.

Problem 2.

1. Show that $5x$ is $o(x^2)$.

2. Show that $2x^2$ is not $o(x^2)$.

3. Show that $1/x$ is $o(x)$.

4. Show that if $f(x)$ is $o(g(x))$, then $f(x)$ is $O(g(x))$.

Problem 3. Compute $s, t \in \mathbb{Z}$ such that $417s + 534t = \gcd(417, 534)$.

Problem 4. Similarly to the division algorithm for integer numbers, there also exists a division algorithm for polynomials (over the real numbers), that finds for any two polynomials $f(x), g(x)$ a polynomial $q(x)$ and a polynomial $r(x)$ with $\deg(r) < \deg(g)$ such that $f(x) = q(x)g(x) + r(x)$. We can use this division to find the greatest common divisor (polynomial) of two polynomials, in an analogous way as for integer numbers. (You can find more detailed explanations e.g. on Wikipedia: Polynomial greatest common divisor.)

1. Let $f(x) = x^4 + 2x^2 - 3$ and $g(x) = x^2 - 1$. What is $f(x)$ divided by $g(x)$?

2. Let $f(x) = 3x^8 + 2x^3 - 1$ and $g(x) = x^2 + 1$. Find $q(x), r(x)$ with $\deg(r) < \deg(g)$ such that $f(x) = q(x)g(x) + r(x)$.

3. Compute the greatest common divisor of $f(x) = x^4 + 2x^2 - 3$ and $g(x) = 3x^5 - 3x^3 + 5x^2 - 5$.

Problem 5. Let $p$ be a prime number and $p(x)$ be a polynomial of degree $n$. 


1. Show that the polynomial $x^2 - 1$ modulo $p$ has two roots. What are the two roots?

2. Find a general description for $p(x)$, such that it has roots $\alpha_1, \alpha_2, \ldots, \alpha_n$ modulo $p$.

3. Find an example where $p(x)$ has less than $n$ roots modulo $p$.

4. Let $m$ be a positive non-prime integer. Find an example where $p(x)$ has more than $n$ roots modulo $m$.

**Problem 6.** Wilson’s theorem states that a natural number $n > 1$ is a prime number if and only if

\[(n - 1)! \equiv -1 \pmod{n}.
\]

Prove the “only-if”-part of this theorem by using Fermat’s little theorem. Moreover you may use the fact that any polynomial of degree $k$ modulo a prime $p$ can have at most $k$ roots.