Introduction to Homomorphic Cryptosystems
Exercise Sheet 9: Polynomial Approximation

Task 1 – Homomorphic Taylor Series

Another approach to calculating homomorphic functions is polynomial approximations such as the Taylor series. The Taylor series approximates a function f around a development point x_o by determining the corresponding polynomial $TS_f(x) = \sum_{n=0}^{m} \frac{f^{(n)}(x_o)}{n!}(x - x_o)^n$. Where $f^{(n)}$ stands for the n-th derivative of the function f. In the following, we will compare how the Taylor series behaves in comparison to the Newton-Raphson method for calculating the root and inverse function.

Note: For the comparison you don't need to implement the approaches homomorphically.

a) To approximate the root function *sqr* using the Taylor series, we must determine the corresponding polynomial TS_{sqr} around the development point x_{sqr}.

   i) Calculate the polynomial TS_{sqr} in general if the highest allowed degree is x^3.

   ii) Determine the concrete polynomial TS_{sqr} for the development point $x_o = 10$ if the highest allowed degree is x^3.

   iii) Using the previously determined polynomial, calculate the root function for the values $\{5.0, 5.1, ...14.9, 15.0\}$. Next, calculate the root function for the same values using the Newton-Raphson method (you can assume the following interval for the Newton-Raphson method: $[5; 15]$). Finally, plot the results of the two methods for calculating the root for the values $\{5.0, 5.1, ...14.9, 15.0\}$ in the same diagram.

b) Repeat task a) and increase the permitted degree in steps of one up to 8.

c) To approximate the root function *inv* using the Taylor series, we must determine the corresponding polynomial TS_{inv} around the development point x_{inv}.

   i) Calculate the polynomial TS_{inv} in general if the highest allowed degree is x^3.

   ii) Determine the concrete polynomial TS_{inv} for the development point $x_o = 10$ if the highest allowed degree is x^3.

   iii) Using the previously determined polynomial, calculate the inverse function for the values $\{5.0, 5.1, ...14.9, 15.0\}$. Next, calculate the root function for the same values using the Newton-Raphson method (you can assume the following interval for the Newton-Raphson method: $[5; 15]$). Finally, plot the results of the two methods for calculating the inverse for the values $\{5.0, 5.1, ...14.9, 15.0\}$ in the same diagram.

d) Repeat task c) and increase the permitted degree in steps of one up to 8.