Tutorial 1: Algebraic tools

I Extended Euclidean Algorithm

The greatest common divisor of two integers $a$ and $b$ can be computed via the fact seen in the lecture. However, computing a gcd by first obtaining the prime factorization of the given numbers does not result in an efficient algorithm, as the problem of factoring integers appears to be difficult. The Euclidean Algorithm is an efficient algorithm for computing the greatest common divisor of two integers that does not require the factorization of the integers. It is based on the following fact:

Fact 1. If $a$ and $b$ are positive integers with $a \geq b$, then $\text{gcd}(a, b) = \text{gcd}(b, a \mod b)$

1. prove the above fact.

2. write the Euclidean Algorithm that computes the gcd of two integers.

3. compute the gcd(4864, 3458).

4. The Euclidean algorithm can be extended so that it does not only yield the greatest common divisor of two integers $a$ and $b$, but also integers $a$ and $b$ satisfying $ax + by = \text{gcd}(a, b)$. We first notice that the Euclidean Algorithm calculates a sequence defined by a two term recurrence:

$$a_0 = a, a_1 = b, a_{n-1} = q_n a_n + a_{n+1}$$

where $q_n = \lfloor \frac{a_{n-1}}{a_n} \rfloor$.

In other terms:

$$a_{n+1} = -q_n a_n + a_{n-1}$$

Now, we consider the sequences $(x_n)$ and $y_n$ defined by:

$$x_0 = 1, x_1 = 0, x_{n+1} = -q_n x_n + x_{n-1}$$

$$y_0 = 0, y_1 = 1, y_{n+1} = -q_n y_n + y_{n-1}$$
• prove, by induction, that \( a_n = ax_n + by_n \).
• write the Extended Euclidean Algorithm that computes the gcd of two integers \( a \) and \( b \) in addition to two integers \( x \) and \( y \) such that \( ax + by = \gcd(a, b) \).
• example: \( a=4864, b=3458 \).

II Congruence relation

Prove that the relation congruent modulo \( n \) partitions \( \mathbb{Z} \) into \( n \) sets.

III EEA and the inverse computation

1. Compute the gcd of \( a = 2^{24} - 1 \) and \( b = 2^{11} - 1 \) and find integers \( x \) and \( y \) such that \( ax + by = \gcd(a, b) \)(you can use any programming language of your choice). Conclude.
2. Application: compute the inverse of \((2^{11} - 1) \mod (2^{24} - 1)\)
3. Generalization: let \( m \) and \( n \) be two integers such that \( n > m \). Prove that \( \gcd(2^n - 1, 2^m - 1) = 2^{\gcd(m, n)} - 1 \). 
   **Hint:** prove first that \((2^n - 1) \mod (2^m - 1) = 2^n \mod m - 1\), then conclude with the Euclidean algorithm.

IV Division with remainder in a ring

Do the following division:

1. \(3x^{13} + 2x^{10} - x^5 + 3x^2 + 1 \) by \( x^7 + 3x^5 + 4 \) in the ring \((\mathbb{Z}[x], +, \times)\)
2. \(x^{13} + x^5 + x^2 + 1 \) by \( x^7 + x^5 \) in the ring \((\mathbb{Z}_2[x], +, \times)\)

V Operations in a polynomial ring

1. Let \( R_1 = (\mathbb{Z}_2[x]/\langle m \rangle, +, \times) \) where \( m = x^8 + x^4 + x^3 + x + 1 \), and let \( a = x^7 + x^4 + x^3 + x + 1 \) and \( b = x^7 + x^6 + x^3 + x^2 + 1 \). Compute \( ab \) and \( \text{inv}(a) \) in \( R_1 \).
2. Let \( R_2 = (\mathbb{Z}_2[x]/\langle x^8 + 1 \rangle, +, \times) \).
   • Is \( R_2 \) a field? justify.
   • Compute \( x^i \) in \( R_2 \), \( 0 \leq i \leq 14 \)