1. Prove the formulas

\((a \mod n) + (b \mod n)) \mod n = (a + b) \mod n,\)
\((a \mod n)(b \mod n)) \mod n = (ab) \mod n.\)

2. Find the elements with multiplicative inverses in \(\mathbb{Z}_{16}\). What are those inverses?

3. The input of the Extended Euclidean algorithm consists of integers \(a\) and \(b\). The algorithm returns a triple \((d, x, y)\) which satisfies the equation \(d = \gcd(a, b) = ax + by\). The recursive version of the algorithm is short:

\textbf{Extended-Euclid}(a, b):

1. if \(b = 0\) then return \((a, 1, b)\);
2. \((d', x', y') := \text{Extended-Euclid}(b, a \mod b)\);
3. \((d, x, y) := (d', y', x' - \lfloor a/b \rfloor y')\);
4. return \((d, x, y)\).

The following example shows how the algorithm works when the input is \(a = 99, b = 78\):

<table>
<thead>
<tr>
<th></th>
<th></th>
<th>(\lfloor a/b \rfloor)</th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>99</td>
<td>78</td>
<td>1</td>
<td>3</td>
<td>-11</td>
<td>14</td>
</tr>
<tr>
<td>78</td>
<td>21</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>-11</td>
</tr>
<tr>
<td>21</td>
<td>15</td>
<td>1</td>
<td>3</td>
<td>-2</td>
<td>3</td>
</tr>
<tr>
<td>15</td>
<td>6</td>
<td>2</td>
<td>3</td>
<td>1</td>
<td>-2</td>
</tr>
<tr>
<td>6</td>
<td>3</td>
<td>2</td>
<td>3</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>3</td>
<td>0</td>
<td>-</td>
<td>3</td>
<td>1</td>
<td>0</td>
</tr>
</tbody>
</table>

Simulate the algorithm with numbers \(a = 210\) and \(b = 715\). How is it possible, with the help of the algorithm, to determine the multiplicative inverse of \(a\) modulo \(p\) (\(p\) a prime)?
4. The following algorithm computes the value \( a^b \mod n \), when \( a, b \) and \( n \) (integers) are given as an input. Number \( b \) is represented in its binary form \( b_k b_{k-1} \cdots b_0 \).

1. \( c := 0; \ f := 1; \)
2. for \( i := k \) downto 0 do {
3. \( c := 2 \times c; \)
4. \( f := (f \times f) \mod n; \)
5. if \( b_i = 1 \) then {
6. \( c := c + 1; \)
7. \( f := (f \times a) \mod n; \}
8. return \( f. \)

Simulate the algorithm with the numbers \( a = 3, \ b = 13, \ n = 4. \)

5. Find the primitive roots of 17.

6. This exercise must be returned either on paper or through email to the lecturer. The deadline is Wednesday, November 6, at 12 noon.

Construct (addition and multiplication tables) the finite field \( GF_f(2^3) \) using the irreducible polynomial \( f(X) = X^3 + X + 1 \). Also construct \( GF_g(2^3) \) using \( g(X) = X^3 + X^2 + 1 \).

Can you define a mapping \( h : GF_f(2^3) \rightarrow GF_g(2^3) \) such that \( h \) is bijective (one-to-one) and \( h \) satisfies the conditions

i) \( h(p(X) \oplus_f q(X)) = h(p(X)) \oplus_g h(q(X)), \)

ii) \( h(p(X) \otimes_f q(X)) = h(p(X)) \otimes_g h(q(X)), \)

for all \( p(X), q(X) \in GF_f(2^3) \). Such a function \( h \) is called an isomorphism and its existence shows that the fields \( GF_f(2^3) \) and \( GF_g(2^3) \) are structurally the same.