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 $\mathbb{Z}_{16}$.

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:

**Extended-Euclid$(a, b)$:**

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

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

<table>
<thead>
<tr>
<th>$a$</th>
<th>$b$</th>
<th>$\lfloor a/b \rfloor$</th>
<th>$d$</th>
<th>$x$</th>
<th>$y$</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 $b_k b_{k-1} \cdots b_0$.

\begin{enumerate}
  \item $c := 0$; $f := 1$;
  \item for $i := k$ downto 0 do 
    \begin{enumerate}
      \item $c := 2 \times c$;
      \item $f := (f \times f) \mod n$;
      \item if $b_i = 1$ then 
        \begin{enumerate}
          \item $c := c + 1$;
          \item $f := (f \times a) \mod n$;
        \end{enumerate}
    \end{enumerate}
  \item return $f$.
\end{enumerate}

Simulate the algorithm with the numbers $a = 3$, $b = 13$, $n = 4$.

5. Find the primitive roots of 17.

6. The following algorithm generates an irreducible polynomial in modular arithmetics. The greatest common divisor (gcd) can be calculated with the help of the Extended Euclidean algorithm.

\textbf{Input}: A prime $p$ and $n \in \mathbb{N}$.

\textbf{Output}: Random monic (leading coefficient is 1) irreducible polynomial of degree $n$ and coefficients are modulo $p$ numbers.

\begin{enumerate}
  \item randomly choose a monic polynomial $P$ of degree $n$ with coefficients modulo $p$ integers.
  \item for $i = 1, \ldots, \lfloor n/2 \rfloor$ do
    \begin{enumerate}
      \item $g_i \leftarrow \gcd(X^{p^i} - X, P)$; if $g_i \neq 1$ then goto 1;
    \end{enumerate}
  \item return $P$.
\end{enumerate}

Generate an irreducible polynomial $P \in \mathbb{Z}_3[X]$ of degree 2 and an irreducible polynomial $Q \in \mathbb{Z}_5[X]$ of degree 3 using the above algorithm.