Algorithmic Number Theory - List 2

Task 1 (15 pts)
Implement the *binary extended gcd algorithm* (Algorithm 14.61 from `https://cacr.uwaterloo.ca/hac/about/chap14.pdf`).

Task 2 (5 pts)
On the basis of the *binary extened gcd algorithm* implement a function that

- takes two arguments m and a such that $m \in \mathbb{N} \setminus \{0, 1\}$, $a \in \{1, 2, \ldots, m-1\}$, and where $\gcd(a, m) = 1$ (when implementing the function, assume that the conditions are satisfied),
- returns $b \in \{1, 2, \ldots, m-1\}$ such that $b \equiv a^{-1} \bmod m$.

Prove that your implementations are correct by implementing tests.