Mandatory Assignment 1a: Computations in Elementary Number Theory

The deadline is Tuesday, September 13 midnight. You have to hand in a short description of the algorithms you implemented, the implementation code as a collection of subroutines (functions), and computational results.

1. Implement Extended Euclidean Algorithm. Let

   $$a = 620709603821307061, b = 390156375246520685$$

   find $d = gcd(a, b)$ and integers u, v such that $d = ua + vb$.

2. Implement binary exponentiation modulo n. Compute $b = a^m \bmod n$ for $(a, m, n) = (393492946341, 103587276991, 72447943125)$.

3. Implement elimination algorithm (reduce the matrix to a row echelon form) to solve the system of linear congruences: factor $n = 456995412589$ or find a solution to

   $$\begin{pmatrix} 1 & -2 & -2 & -2 & -1 \\ 0 & 3 & -2 & -3 & 1 \\ 3 & 0 & 0 & 1 & -1 \\ 3 & -3 & -2 & 0 & 1 \\ 0 & -3 & 3 & -3 & -3 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \end{pmatrix} \equiv \begin{pmatrix} 2 \\ 3 \\ 2 \\ 1 \\ 2 \end{pmatrix} \bmod n.$$

4. Implement the algorithm to compute Jacobi symbol (a/n), where a is an integer and n is an odd positive integer. Compute

   $$(-776439811/50556018318800449023).$$

5. Implement Solovay-Strassen test to check the primality of an odd positive integer n. Prove that $n = 2^{127} - 1$ is a probable prime with error probability $< 1/2^{20}$.