1. Consider ElGamal Public-key Cryptosystem in Galois field $GF(2^4)$ with polynomial $x^4 + x + 1$ and with the primitive element $\alpha = 0010 = x$. Your private key is $a = 7$.
   a) Compute your public key $\beta$.
   b) Decrypt ciphertext (0100,1110) using your secret key.

2. It is given that
   \[ 12^{2004} \equiv 4815 \pmod{50101}, \]
   where 50101 is a prime. Show that the element $\alpha = 4815$ is of order 25 in the multiplicative group $\mathbb{Z}_{50101}^\times$.

3. Using Shanks’ algorithm attempt to determine $x$ such that
   \[ 4815^x \equiv 48794 \pmod{50101}. \]
   Hint: See Problem 2.

4. Element $\alpha = 202$ is of order 16 in the multiplicative group $\mathbb{Z}_{2005}^\times$. It is given that element $\beta = 133$ is in the subgroup generated by $\alpha$. Using Shanks’ algorithm compute the discrete logarithm $x$ of $\beta = 133$ to the base $\alpha = 202$, that is, solve the congruence
   \[ 202^x \equiv 133 \pmod{2005}. \]

5. Solve the congruence
   \[ 3^x \equiv 135(\pmod{353}) \]
   using the Pohlig-Hellman algorithm.

6. Let $E$ be the elliptic curve $y^2 = x^3 + x + 13$ defined over $\mathbb{Z}_{31}$.
   a) Determine the quadratic residues modulo 31.
   b) Determine the points on $E$.

7. Let $p$ be prime and $p > 3$. Show that the following elliptic curves over $\mathbb{Z}_p$ have $p + 1$ points:
   a) $y^2 = x^3 - x$, for $p \equiv 3(\pmod{4})$. Hint: Show that from the two values $\pm r$ for $r \neq 0$ exactly one gives a quadratic residue modulo $p$.
   b) $y^2 = x^3 - 1$, for $p \equiv 2(\pmod{3})$. Hint: If $p \equiv 2(\pmod{3})$, then the mapping $x \mapsto x^3$ is a bijection in $\mathbb{Z}_p$. 