CS 402 Cryptography

Problem Sheet 9

(1) (i) Let p be an odd prime. Given $\beta \equiv \alpha^x \bmod p$, where α is a primitive element mod p and $0 \leq x < p-1$, explain how to decide whether the unknown x is even or odd.

(ii) Apply the Pohlig-Hellman algorithm to calculate the discrete log of 12 to the base 7 in $\mathbb{Z}_{41}$.

(iii) Comment on the efficiency of the Pohlig-Hellman algorithm.

(2) Given that $3^6 \equiv 44 \bmod 137$, and $3^{10} \equiv 2 \bmod 137$, solve $3^x \equiv 11 \bmod 137$.

(3) Let p be a prime and $a \in \mathbb{Z}$. Define the Legendre symbol $\left(\frac{a}{p}\right)$. Prove that

(i) $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$,

(ii) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.

(4) Using properties of Jacobi symbols, determine whether or not 7411 is a quadratic residue mod the prime 9283.