T-79.503 Foundations of Cryptology
Homework 11
November 26, 2003

1. Consider the *ElGamal Public-key Cryptosystem* in the finite field $\mathbb{Z}_2[x]/(x^3+x+1)$. The private key is $a = 3$ and the primitive element is $\alpha = \texttt{010}$. Compute the public key β, and decrypt the ciphertext $(\texttt{110}, \texttt{110})$.

2. Solve the congruence
$$3^x \equiv 24 (\bmod 31)$$
using
   a) Shanks' algorithm; and
   b) the Pohlig-Hellman algorithm.

3. Solve the congruence
$$3^x \equiv 135 (\bmod 353)$$
using the Pohlig-Hellman algorithm.

4. (Stinson 6.4 (a)) Suppose that p is an odd prime and k is a positive integer. The multiplicative group $\mathbb{Z}^*_{p^k}$ has order $\phi(p^k) = p^{k-1}(p-1)$, and is known to be cyclic. A generator of this group is called a *primitive element modulo* p^k. Suppose that α is a primitive element modulo p. Prove that at least one of α or $\alpha + p$ is a primitive element modulo p^2.

5. 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.

6. 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 $p \equiv 3(\text{mod}4)$. Hint: Show that from the two values $\pm r$ for $x \neq 0$ exactly one gives a quadratic residue modulo p.
   b) $y^2 = x^3 - 1$, for $p \equiv 2(\text{mod}3)$. Hint: If $p \equiv 2(\text{mod}3)$, then the mapping $x \mapsto x^3$ is a bijection in $\mathbb{Z}_p$.