T-79.5501 Cryptology
Homework 12
April 24, 2007

1. Let E be the elliptic curve $y^2 = x^3 + 2x + 7$ defined over $\mathbb{Z}_{31}$.
   a) Determine the quadratic residues modulo 31.
   b) Determine the points on E.

2. Let E be as above. Compute the decompressions of $(18, 1)$, $(3, 1)$, $(17, 0)$ and $(28, 0)$.

3. (Stinson 6.17, see also Problems 1 and 2) Let E be the elliptic curve $y^2 = x^3 + 2x + 7$ defined over $\mathbb{Z}_{31}$. It can be shown that $\#E = 39$ and $P = (2, 9)$ is an element of order 39 in E. The *Simplified ECIES* defined on E has $\mathbb{Z}_{31}^*$ as its plaintext space. Suppose the private key is $m = 8$.
   a) Compute $Q = mP$.
   b) Decrypt the following string of ciphertext:

$$((18, 1), 21), ((3, 1), 18), ((17, 0), 19), ((28, 0), 8)$$

4. 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 $r \neq 0$ 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 $\mathbb{Z}_p$.

5. (Stinson 6.18) In elliptic curves computing $-P$ given a point P is trivial, compared to finite multiplicative groups based on fields where the analogical operation is taking inverses (using the Euclidean algorithm). By this property the double-and-add algorithm for point multiplication can be speeded up by using a NAF representation of the multiplier (see Section 6.5.5).
   a) Determine the NAF representation of the integer 87.
   b) Using the NAF representation of 87, use Algorithm 6.5 to compute $87P$, where $P = (2, 6)$ is a point on the elliptic curve $y^2 = x^3 + x + 26$ defined over $\mathbb{Z}_{127}$. Show the partial results during each iteration of the algorithm.