

Exercise 7

TMA4160 Cryptography, autumn 2007

Task 1.

a) Given the elliptic curve over \mathbf{Z}_{11} defined by $y^2 = x^3 + 3x + 7$, and the point $P = (8, 9)$, find $2P$, $5P$ and $10P$.

b) Use Hasse's theorem (on page 261 in Stinson's book) to find the exact number of points on the curve.

c) Find all the points on the curve.

Task 2.

a) (Repetition from your algebra-class) Describe all abelian groups with exactly 100 elements, up to isomorphism. For each of the groups, what is the maximal order of an element?

b) Assume there is an elliptic curve over \mathbf{Z}_{107} which as an abelian group $(E, +)$ has 100 elements. Use Theorem 6.1 on page 261 in Stinson's book to show that there is an element of order 50.

Task 3. Consider an arbitrary polynomial of degree three, $f(y) = x^3 + cx^2 + ax + b$. Show that, using a proper linear substitution, we can assume $c = 0$. (Here assume that the coefficients are either real numbers, or numbers in \mathbf{Z}_p with $p \neq 3$.)

Task 4. Show that any elliptic curve over \mathbf{Z}_{83} has an element of order > 30 .