

Exercise 8

TMA4160 Cryptography, autumn 2007

Task 1.

a) Let $(G, +)$ be an abelian group. Let H be the subset of all elements x in G with $x + x = 0$. Show that H is a subgroup. If G is cyclic, what is the maximal order of H ?

b) Let $p \neq 3$ be prime and $(E, +)$ an elliptic curve defined by $y^2 = x^3 + ax + b$, with the property that $x^3 + ax + b$ has three distinct roots in \mathbf{Z}_p . Show that $(E, +)$ is not cyclic.

c) For some p , find an example of an elliptic curve with the property described in b).

The exercises below are all from Stinson's book "Cryptography, Theory and Practice", 3rd edition.

Task 2. Exercise 6.13

Task 3. Exercise 4.3

Task 4. Exercise 1.18