Introduction to mathematical cryptography
Homework problems
Week 12

23. Let $p > 3$ be a prime number, and let $y^2 = x^3 + Ax + B$ be an equation defining an elliptic curve. Prove that $4A^3 + 27B^2 \neq 0$ implies that the cubic polynomial $x^3 + Ax + B$ has no multiple roots.

24. Let $p > 3$ be a prime number. Prove that an elliptic curve over $\mathbf{F}_p$ has at most $2p + 1$ points. (The proof must be elementary, e.g. you cannot refer to Hasse's theorem.)

Note: Please provide complete arguments everywhere.