Homework 8
Math 124, Fall 2005
Due Wednesday, November 16th

No late assignments will be accepted.

1. Show that \((3, 8)\) is a torsion point of order 7 on \(y^2 = x^3 - 43x + 166\).

2. Consider the ring \(\mathbb{Q}[x]\) of polynomial with rational coefficients.
   (a) Define an Euclidean division algorithm on \(\mathbb{Q}[x]\) using the degree of a polynomial as the Euclidean norm.
   (b) Show that if a ring \(R\) has an Euclidean algorithm and if \(I\) is an ideal\(^1\) of \(R\) then \(I\) is generated by a single element. [Hint: Consider the element of minimal norm in \(I\).]
   (c) Prove that for any complex number \(\alpha\)
   \[
   I_\alpha = \{ f \in \mathbb{Q}[x] \mid f(\alpha) = 0 \}
   \]
   is an ideal.
   (d) For any algebraic number\(^2\) over \(\mathbb{Q}\), show that there exists a single monic polynomial \(f_\alpha = x^n + \ldots\) such that
   \[
   f_\alpha(\alpha) = 0 \quad g(\alpha) = 0 \implies f_\alpha | g.
   \]
   The polynomial \(f_\alpha\) is called the **minimal polynomial** of \(\alpha\). The other zeros of \(f_\alpha\) are the **algebraic conjugate** of \(\alpha\). They have the same minimal polynomial.
   (e) Show that if \(\alpha\) and \(\alpha'\) are algebraic conjugates then
   
   \[
   g(\alpha) = 0 \iff g(\alpha') = 0
   \]
   (f) Show that for any \(\alpha \in \mathbb{C}\), \(\alpha\) and \(\bar{\alpha}\) are algebraic conjugates.
   (g) Show that \(\alpha\) is rational if and only if \(\alpha\) has no algebraic conjugates other than itself. [Hint : You might want to show that if \((x - \alpha)^n\) is a rational polynomial then \(\alpha\) itself is rational.]
   (h) Find all algebraic conjugates of \(\sqrt[3]{2}\).
   (i) Show that a rational polynomial of degree 3 has either zero, one or three rational solutions. Show that each of these three possibilities can happen.

**Remark 1.** We have used this last fact to show that if \(P\) and \(Q\) are two rational points on an elliptic curve then so is \(P + Q\).

---

\(^1\) An ideal is a subset that is closed under addition and under multiplication by elements of \(R\).
\(^2\) \(\alpha\) is algebraic over \(\mathbb{Q}\) if there is a polynomial \(f(x)\) in \(\mathbb{Q}[x]\) which has \(\alpha\) as a zero.