D-MATH
Prof. Brent Doran

Algebra II

FS 2014

Serie 4

Factoring integer polynomials

1. (Lagrange interpolation) Let $a_0, \dots, a_d$ and $b_0, \dots, b_d$ be elements of a field F. and suppose that the a_i are distinct. Exhibit a polynomial $g(x) \in F[x]$ of degree $\leqslant d$ that satisfies $g(a_i) = b_i$ for each $0 \leqslant i \leqslant d$. Then prove that a polynomial with these properties is unique.

2. (Eisenstein criterion) Let R be a unique factorisation domain with field of fractions $\mathcal{F}$. Let $f(x) = a_n x^n + \cdots + a_0$ be a polynomial in $R[x]$ and let $\mathfrak{P}$ be a prime ideal in R. If
$$a_n \notin \mathfrak{p}, \quad a_i \in \mathfrak{p} \text{ for every } 0 \leqslant i \leqslant n-1, \quad a_0 \notin \mathfrak{p}^2,$$
then $f(x)$ is irreducible in $\mathcal{F}[x]$.
   (a) When is a principal ideal prime ? When is a maximal ideal prime ?
   (b) Prove the statement for $R = \mathbb{Z}$.
   (c) Find, for every $n \in \mathbb{N}$, an irreducible integer polynomial of degree n.

3. Factor the following polynomials into irreducible factors.
   (a) $x^3 + x + 1$ in $\mathbb{F}_p[x]$, for $p = 2, 3, 5$.
   (b) $x^4 + x + 1$ in $\mathbb{Q}[x]$.
   (c) $x^3 + 2x^2 - 3x + 3$ in $\mathbb{Q}[x]$.
   (d) $x^{p-1} + x^{p-2} + \cdots + 1$ in $\mathbb{Q}[x]$ where p is a prime. (**Hint** : Consider the substitution $x = y + 1$.)