MATH 371 – Homework 7– November 1, 2013

1. I'm not sure what I was thinking with problem 3(c) last week, so let's try it again — for some values of k the polynomial $x^k + x + 1$ is irreducible in $\mathbb{Z}[x]$ but for other values of k it's not. Which are which? Proof?

---

2. Prove that one of 2, 3 or 6 is a square in $\mathbb{F}_p$ for every prime p. Conclude that the polynomial

$$x^6 - 11x^4 + 36x^2 - 36 = (x^2 - 2)(x^2 - 3)(x^2 - 6)$$

has a root mod p for every p but has no root in $\mathbb{Z}$.

---

3. (a) Show that the polynomial $x^p - x - a$ is irreducible in $\mathbb{F}_p[x]$ for any $a \in \mathbb{F}_p$ provided $a \neq 0$.

(b) Let $\alpha = [x]$ in $E = \mathbb{F}_p[x]/\langle x^p - x - a\rangle$ and show that the mapping $\varphi\colon E \to E$ which takes 1 to 1 and α to $\alpha + 1$ is an automorphism of E that fixes $\mathbb{F}_p$. Then show that this automorphism generates a cyclic group of automorphisms of E over $\mathbb{F}_p$.

---

4. Find implicit equations for the affine varieties parametrized as follows:

(a) In $\mathbb{R}^4$: $x_1 = 2t_1 - 5t_2$, $x_2 = t_1 + 2t_2$, $x_3 = -t_1 + t_2$, $x_4 = t_1 + 3t_2$.

(b) In $\mathbb{R}^3$: $x = t$, $y = t^4$, $z = t^7$

---

5. Show that all polynomial parametric curves in k^2 (k a field) are contained in affine algebraic varieties as follows:

(a) Show that the number of distinct monomials $x^a y^b$ of total degree $\leqslant m$ in $k[x, y]$ is equal to $(m + 1)(m + 2)/2$.

(b) Show that if $f(t)$ $g(t)$ are polynomials of degree $\leqslant n$ in t, then for m large enough, the "monomials" $[f(t)]^a[g(t)]^b$ with $a + b \leqslant m$ are linearly dependent.

(c) Deduce that if C is the polynomial parametric curve in k^2 given by $x = f(t)$, $y = g(t)$, then C is contained in $\mathbf{V}(F)$ for some $F \in k[x, y]$.

(d) Generalize the above to show that any polynomial parametric surface in k^3 given by $x = f(t, u)$, $y = g(t, u)$, $z = h(t, u)$ is contained in an algebraic surface $\mathbf{V}(F)$ for some $F \in k[x, y, z]$.