Dartmouth College

Mathematics 81/111 — Homework 3

1. Given two relatively prime polynomials in $\mathbb{C}[x,y]$, Bézout's theorem in algebraic geometry gives the product of their degrees as an upper bound for the number of points of intersection. For example in $\mathbb{R}^2$ we expect the parabola $y - x^2 = 0$ will intersect a circle $x^2 + (y-a)^2 - 4 = 0$ in anywhere from 0-4 points (but no more than 4), depending on the value of a.

   In this problem we give a first approximation to Bézout's theorem by proving that given two relatively prime polynomials $f(x,y)$, $g(x,y)$ in $k[x,y]$ (k a field), their zero sets (i.e., the set of points (x,y) where $f(x,y) = 0 = g(x,y)$) is finite.

   (a) Let A be a UFD with field of fractions K. Let $f, g \in A[x]$. Show that f, g are relatively prime in $A[x]$ if and only if f, g are relatively prime in $K[x]$ and their contents, $C(f)$ and $C(g)$, are relatively prime in A.

   (b) Let k be a field and $f, g \in k[x,y]$ be relatively prime. Show that the set of points (x,y) where $f(x,y) = 0 = g(x,y)$) is finite.

2. Let $n \geq 1$ and consider the polynomial $f(x,y) = y^n - (x^3 - x) \in \mathbb{Q}[x,y]$.

   (a) Characterize the quotient $\mathbb{Q}[x,y]/(y, f(x,y))$ in terms of familiar rings.

   (b) Show that $A = \mathbb{Q}[x,y]/(f)$ is an integral domain containing an isomorphic copy of $\mathbb{Q}[x]$. Show moreover that A is finitely generated $\mathbb{Q}[x]$-module, in particular, that $A \subseteq \mathbb{Q}[x](1 + (f)) + \mathbb{Q}[x](y + (f)) + \cdots + \mathbb{Q}[x](y^{n-1} + (f))$.

   (c) Show that $B = \mathbb{Q}[x,y]/(x, f(x,y))$ is an integral domain if and only if $n = 1$, but in any case is a finite dimensional vector space over $\mathbb{Q}$.

3. Let A be a commutative ring with identity having prime characteristic p, and let $\varphi : A \to A$ be the map $\varphi(a) = a^p$. The map φ is called the *Frobenius map*.

   (a) Show that φ is a ring homomorphism.

   (b) Henceforth assume that the ring A is specialized to a field F (having characteristic p). Show that $\varphi : F \to F$ is injective.

   (c) Show that if F is a finite field, then φ is surjective.

   (d) Show that if F is a finite field, then for any $f \in F[x]$, there exists a $g \in F[x]$ with $f(x^p) = (g(x))^p$.

   (e) Show that if $F = \mathbb{Z}/p\mathbb{Z}$, then φ is the identity map, and that for any $f \in F[x]$, $f(x^p) = (f(x))^p$.

(continued on next page)

4. Hint: If you don't know where to begin, I would suggest looking up diagonalizable in Lang's index. The reference will give (as a homework problem) an important theorem.

   (a) Let A be an $n \times n$ matrix over the complex numbers, $\mathbb{C}$, for which $A^k = I_n$ is the identity matrix for some integer $k \geq 1$. Show that A is diagonalizable.

   (b) Let F be a field of prime characteristic p, and $A = \begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix} \in M_2(F)$. Show that $A^p = I_2$, and that A is diagonalizable if and only if $\alpha = 0$.

5. We have seen a number of tests to help determine whether a polynomial is irreducible, and they will serve you well. On the other hand, neither one size nor one tool fits all problems.

   (a) Show that for all $n \geq 1$, $f(x) = (x-1)(x-2)\cdots(x-n) - 1$ is irreducible in $\mathbb{Z}[x]$.

   (b) Show that for all $n \geq 1$ (except $n = 4$), $f(x) = (x-1)(x-2)\cdots(x-n) + 1$ is irreducible in $\mathbb{Z}[x]$. This part requires a bit more persistence than the first part.