Math 75 – Homework

Posted May 16, 2014; due Wednesday, May 21, 2014

1. Consider the Euclidean algorithm applied to $a, b \in K[x]$, where K is a field and $\deg a > \deg b \geq 0$. Let
$$r_{-1} = a, \quad r_0 = b, \quad u_{-1} = 1, \quad u_0 = 0, \quad v_{-1} = 0, \quad v_0 = 1.$$
If the r's, u's, and v's have been defined for subscripts smaller than j and $r_j \neq 0$, let q_j be the quotient when r_{j-1} is divided into r_{j-2}, and let
$$r_j = r_{j-2} - q_j r_{j-1}, \quad u_j = u_{j-2} - q_j u_{j-1}, \quad v_j = v_{j-2} - q_j v_{j-1}.$$
This continues until some $r_k = 0$. Prove that the sequence of degrees of the polynomials $r_{-1}, r_0, \ldots, r_{k-1}$ is strictly decreasing, and for the polynomials u_j, v_j, their degrees, starting with $j = 1$, are strictly increasing.

2. With notation as in the previous problem, show that
$$r_{j-1}u_j - r_j u_{j-1} = \pm b, \quad r_{j-1}v_j - r_j v_{j-1} = \pm a, \quad u_{j-1}v_j - u_j v_{j-1} = \pm 1.$$

3. Suppose that K is finite field with $2^k = n + 1$ elements and α is a primitive element of K. Show that if j is a positive integer and $2^{\lfloor k/2 \rfloor} j < n$, then the degree of the minimum polynomial of α^j over $\mathbb{F}_2$ is k. (Hint: Show that α^j has more than $k/2$ conjugates.)

4. With notation as above, show that if $1 \leq i < j$ are odd integers and $2^{\lfloor k/2 \rfloor} j < n$, then the minimum polynomials for α^i and α^j over $\mathbb{F}_2$ are different.

5. With notation as above, show that if $k \geq 3$ and $2t \leq \sqrt{n} + 1$ then the dimension of $\mathrm{BCH}(k, t)$ is $n - tk$.