Math 114 Professor K. Ribet

Homework assignment #15 due May 11, 2004

Let F be a finite field; write q for the number of elements of F. Let n be a positive integer. Show that the polynomial $t^{q^n} - t \in F[t]$ factors as the product of the monic irreducible polynomials $g(t) \in F[t]$ whose degrees are divisors of n.

For each $d \geq 1$, let $N(d)$ be the number of monic irreducible polynomials in $F[t]$ of degree d. Establish the formula $q^n = \sum_{d|n} N(d)d$ for all d and all n. Show that this formula may be used to compute the numbers $N(d)$ recursively. Illustrate by computing $N(d)$ for $d \leq 10$ when $q = 2$. (In particular, you are finding the number of irreducible degree-10 polynomials over the field with 2 elements.)

Use the formula $q^n = \sum_{d|n} N(d)d$ to write $nN(n)$ as an alternating sum of powers of q; show, more precisely, that we have

$$N(n) = \frac{1}{n} \sum_{d|n} \mu(n/d) q^d,$$

where μ is the Möbius function. For this, you need to use the Möbius inversion formula, which is proved typically in Math 115 and perhaps also in Math 113. Check your Math 113 book or `http://planetmath.org/encyclopedia/MobiusInversionFormula.html` .

Show that $N(n)$ is positive for all n.

Let $p_1, \ldots, p_s$ be distinct prime numbers and let n be a positive integer. Show that there is a monic polynomial $f(t)$ of degree n in $\mathbf{Z}[t]$ so that $f(t)$ is irreducible mod p_i for each $i = 1, \ldots, s$.