HOMEWORK 8

DUE 7 MARCH 2014

1. Factor $x^9 - x$ and $x^{27} - x$ in $\mathbb{F}_3$. Prove that your factorizations are irreducible.

2. Factor $x^{16} - x$ in $\mathbb{F}_4$ and $\mathbb{F}_8$. Prove that your factorizations are irreducible.

3. Let k be a finite field with q elements. Define the *zeta function* of k by

$$Z(u) = (1-u)^{-1} \prod_p (1 - u^{\deg p})^{-1},$$

where p ranges over all monic irreducible polynomials $p = p(X) \in k[X]$.

(a) Prove that $Z(u)$ is a rational function and determine this rational function.

(b) Let $\pi_q(n)$ be the number of primes p as in (a) of degree at most n. Prove that

$$\pi_q(n) \sim \frac{q}{q-1} \frac{q^n}{n} \quad \text{as} \quad n \longrightarrow \infty.$$

Remark: This is the analogue of the prime number theorem in number theory, but it is essentially trivial in the present case, because the Riemann hypothesis is trivially verified. Things get more interesting fast after this case. Consider an equation $y^2 = x^3 + ax + b$ over a finite field $\mathbb{F}_q$ with q elements of characteristic $\neq 2, 3$. Assume $-4a^3 - 27b^2 \neq 0$, in which case the curve defined by this equation is called an *elliptic curve*. Define N_n by

$$N_n - 1 = \text{ number of points } (x, y) \text{ satisfying the above equation with } x, y \in \mathbb{F}_{q^n}$$

(the extension of $\mathbb{F}_q$ of degree n). Define the zeta function $Z(u)$ to be the unique rational function such that $Z(0) = 1$ and

$$\frac{Z'(u)}{Z(u)} = \sum_{n=1}^{\infty} N_n u^{n-1}.$$

A famous theorem of Hasse asserts that $Z(u)$ is a rational function of the form

$$Z(u) = \frac{(1 - \alpha u)(1 - \overline{\alpha} u)}{(1-u)(1-qu)},$$

where α is an imaginary quadratic number (not real, quadratic over $\mathbb{Q}$) and $\alpha\overline{\alpha} = q$, so $|\alpha| = q^{1/2}$. See Hasse, "Abstrakte Bergrundung der komplexen Multiplikation und Riemannsche Vermutung in

Funktionenkörpern," *Abh. Math. Sem. Univ. Hamburg* **10** (1934) pp. 325–348.

From Dummit and Foote: section **13.4** problem 3, 4, 5; section **13.5** problems 6, 11; section **13.6** problems 4, 8, 10, 11.