Math 75 – Homework #4
posted April 18, 2008; due Monday, April 21, 2008

Exercises

1. Show that if q is an integer at least 2, then
$$\frac{1}{d}q^d - \frac{2}{d}q^{d/2} \sim \frac{1}{d}q^d \quad \text{as } d \to \infty,$$
where we say $u(d) \sim v(d)$ as $d \to \infty$ if $\lim_{d\to\infty} u(d)/v(d) = 1$.

2. Give a careful proof, citing the relevant results from the class lecture notes, that $x^{q^d} - x$ is squarefree over a field with q elements if there is an irreducible polynomial over the field of degree d. (In particular, this almost follows from Corollary 2 in Lectures 4&5, so complete the proof for this exercise using other results from those notes. This problem was also discussed in class on April 14.)

3. The proof of Theorem 2 in the Lecture 9 notes gives a way of listing all generators for $F^\times$ if you can find one generator. Construct a finite field with 16 elements, find one generator for the multiplicative group, and then find all the generators.

4. Show that the additive group of a finite field is cyclic if and only if the number of elements in the field is prime. (Note: a group is called *cyclic* if it has a generator.)

5. Decide whether or not the two fields $\mathbb{R}$ and $\mathbb{C}$ (the real numbers and complex numbers, respectively) are isomorphic. If they are isomorphic, give an isomorphism between them. If they are not isomorphic, prove that no isomorphism is possible.

6. Let $F = \mathbb{Z}/(2)$. Set $K = F[x]/(x^3 + x + 1)$ and $L = F[x]/(x^3 + x^2 + 1)$. Then both K and L are 8-element fields, so must be isomorphic, by the main result of Lecture 10. Use the proof of that result to write down an explicit map $\phi\colon K \to L$ which is an isomorphism.

7. If p is a prime and d is a positive integer, show that for each positive divisor j of d there is a unique subfield of $\mathbb{F}_{p^d}$ isomorphic to $\mathbb{F}_{p^j}$ and that $\mathbb{F}_{p^d}$ has no other subfields.