Algebra and Computation (MIT 6.s897) Lecturer: Madhu Sudan
Problem Set 1 Due: Friday, March 6, 2015

Instructions

Goal: The goal of this problem set is to induce some "finite field" thinking. So while it would be great if you can solve the problem without consulting texts, if that makes things better feel free to do so.

Collaboration: Collaboration is allowed, but try to think of the solutions you eventually came up with (possibly collaboratively) in isolation and make sure you understand it (and internalize it).

Writeup: The due date is a recommendation rather than a deadline. It is best if you think of the questions and answers sooner rather than later. The goal of this pset is only to get you to think about potentially weak points in your background. So submission of answers is optional - but I would like to get an email acknowledging that you have thought about the questions and know how to answer them. If you have any questions, email me. If you think you would like to run your solutions by me to verify them or to check if there are alternate solutions, do write them up and send to me by email.

Exercises

1. Prove $\mathbb{F}_q[x]/(g(x))$ is a field of cardinality q^d if and only if g is an irreducible polynomial of degree d.

2. Prove that the multiplicative group of the finite field $\mathbb{F}_q$, denoted $\mathbb{F}_q^*$ is cyclic. Conclude that every field has a primitive element.

3. If ω is a primitive element in $\mathbb{F}_{q^d}$ then prove that ω is a generator of $\mathbb{F}_{q^d}$ over $\mathbb{F}_q$.

4. Let $\alpha \in \mathbb{F}_{q^d}$ have $g \in \mathbb{F}_q[x]$ as it minimal polynomial. Prove that $\mathbb{K} = \mathbb{F}_q[x]/(g)$ is a subfield of $\mathbb{F}_{q^d}$ and so the degree of g divides d.

5. Prove the identity $x^q - x = \prod_{a \in \mathbb{F}_q}(x - a)$.

6. Prove $x^{q^d} - x = \prod_{g \in \mathcal{P}_{q,d}} g(x)$ where

$$\mathcal{P}_{q,d} = \{g \in \mathbb{F}_q[x] | g \text{ irreducible, monic, with } \deg(g) | d\}.$$

7. Prove that if $g \in \mathbb{F}_q[x]$ is irreducible of degree d, then it splits completely in $\mathbb{F}_{q^d}$. (In class we claimed that g has a root in $\mathbb{F}_q[x]/(g)$, and if one combines this with the assertion that fields of cardinality q^d are unique then it follows that $\mathbb{F}_{q^d}$ has a root of $g(x)$. But the way to prove the uniqueness is by proving that g has a root in $\mathbb{F}_{q^d}$.)

8. Prove that there is a unique field of any given cardinality: In particular suppose $g \in \mathbb{F}_p[x]$ is irreducible of degree $a \cdot b$ and $h \in \mathbb{F}_{p^a}[x]$ is irreducible of degree b. Then prove that $\mathbb{F}_p[x]/(g(x)) \cong \mathbb{F}_{p^a}[x]/(h(x))$.

9. Write down the full details of the reduction alluded to in the beginning of Lecture 7 reducing factorization of a polynomial $f \in \mathbb{F}_q[x]$ with all irreducible factors having degree d, to root finding in $\mathbb{F}_{q^d}$.