Winter 2018, Math 148: Week 4 Problem Set
Due: Friday, February 9th, 2018
Finite Fields

Discussion problems. The problems below should be completed in class.

(D1) *Finite fields.* The goal of this problem is to systematically build "small" finite fields.

(a) Suppose $F_3 = \{0, 1, a\}$ is a field with exactly 3 elements. Fill in as much of the addition and multiplication table as you can using only the field axioms.

(b) How many entries in your answer to part (a) remain? Which field(s) can F_3 be?

(c) Do the same for a field $F_4 = \{0, 1, a, b\}$ with exactly 4 elements.

(d) What is the order of each element of F_4? What familiar additive group did you obtain? With this in mind, is the multiplication structure what you expected it to be?

(e) Suppose F_6 is a field with exactly 6 elements. Can $1 \in F_6$ have order 6?

(f) It turns out the order of an element of a finite ring must divide the size of the ring. With this in mind, for each possible order of $1 \in F_6$, try writing out the addition and multiplication tables. When are you able to fill both tables?

(g) Fill in the addition and multiplication tables for a field $F_5 = \{0, 1, a, b, c\}$ with exactly 5 elements (this is tricky, but a fun challenge!). What ring(s) do you get?

(D2) *Constructing finite fields.*

(a) Compare within your group the polynomials you found in $\mathbb{Z}_2[z]$ in problem (P2).

(b) For any finite field F, the set $F \setminus \{0\}$ is a *cyclic* group under multiplication (you proved this on your homework last week for $F = \mathbb{Z}_{13}$). Verify this fact for $\mathbb{F}_4$ (from the preliminary problems) by finding a cyclic generator (i.e. an element $a \in \mathbb{F}_4$ such that every nonzero element of $\mathbb{F}_4$ is a power of a).

(c) A nonzero element of $\mathbb{F}_{p^r}$ is *primitive* if it generates $\mathbb{F}_{p^r} \setminus \{0\}$ as a group under multiplication. Find a primitive element in $\mathbb{F}_7$, $\mathbb{F}_{11}$ and $\mathbb{F}_{41}$.

(d) Using the methods we have developed so far, construct a finite field $\mathbb{F}_9$ with exactly 9 elements. Find a primitive element in $\mathbb{F}_9 \setminus \{0\}$.

(e) Determine which elements of $\mathbb{F}_{32}$ are primitive. Hint: no excessive calculations needed!

(D3) *Factoring over finite fields.* Let $q = p^r$ for p prime and $r \geq 1$.

(a) Factor the polynomial $x^5 - x$ over $\mathbb{F}_5$. Do the same for $x^7 - x$ over $\mathbb{F}_7$.

(b) Factor the polynomial $x^4 - x$ over $\mathbb{F}_4$. Hint: use a variable other than x (such as z) when writing elements of $\mathbb{F}_4$.

(c) Formulate a conjecture for how $x^q - x$ factors over $\mathbb{F}_q$ (you don't have to prove it!).

(d) Factor $x^4 - x$ and $x^8 - x$ over $\mathbb{Z}_2$. Hint: look at your answer to problem (D2) part (a).

(e) Factor $x^9 - x$ over $\mathbb{Z}_3$. Hint: find some low-degree irreducible polynomials over $\mathbb{Z}_3$.

(f) Formulate a conjecture about how $x^{p^n} - x$ factors over $\mathbb{Z}_p$ (proof not required!).

(g) Factor $x^8 - x$ over $\mathbb{F}_4$. Does this hint at an extension of your conjecture from part (f)?

Required problems. As the name suggests, you must submit *all* required problem with this homework set in order to receive full credit.

(R1) Factor $f(x) = x^5 + x^4 + 1$ over $\mathbb{F}_2$, $\mathbb{F}_4$, and $\mathbb{F}_8$.

(R2) Multiply all of the nonzero elements of $\mathbb{F}_5$ together. Do the same for $\mathbb{F}_{11}$ and $\mathbb{F}_4$. Find a formula for the product of all nonzero elements of $\mathbb{F}_{p^r}$.

(R3) For p prime, find a formula for the number of irreducible polynomials of degree at most 3 in $\mathbb{Z}_p[x]$. You are *not* required to prove your formula holds.

(R4) Provide a proof for either (R2) or (R3). Bonus points will be awarded if you prove both. Hint: use the theorem about how $x^q - x$ factors over $\mathbb{F}_q$.

Selection problems. You are required to submit all parts of *one* selection problem with this problem set. You may submit additional selection problems if you wish, but please indicate what you want graded. Although I am happy to provide written feedback on all submitted work, no extra credit will be awarded for completing additional selection problems.

(S1) (a) Let $a(n)$ denote the number of degree-n irreducible polynomials over $\mathbb{F}_2$. Prove that

$$2^n = \sum_{d|n} d \cdot a(d).$$

Hint: use the theorem about how $x^{2^d} - x$ factors over $\mathbb{F}_2$.

(b) Find the number of irreducible polynomials over $\mathbb{F}_2$ with degree exactly 31.

(c) Find the number of irreducible polynomials over $\mathbb{F}_2$ with degree exactly 21.

(S2) A field F is *algebraically closed* if every polynomial in $F[x]$ has a root in F. For example, $\mathbb{C}$ is algebraically closed, but $\mathbb{R}$ is not since $x^2 + 1$ has no roots in $\mathbb{R}$. Prove that no finite field $\mathbb{F}_{p^r}$ is algebraically closed.

Challenge problems. Challenge problems are not required for submission, but bonus points will be awarded for submitting a partial attempt or a complete solution.

(C1) By the fundamental theorem of finite fields,

$$F = \mathbb{Z}_2[z]/\langle z^3 + z + 1\rangle \qquad \text{and} \qquad F' = \mathbb{Z}_2[z]/\langle z^3 + z^2 + 1\rangle$$

are both fields with 8 elements and thus must be the same. Find an explicit bijection $F \to F'$ that preserves both addition and multiplication.