Winter 2017, Math 148: Week 4 Problem Set
Due: Wednesday, February 8th, 2017
Finite Fields

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

(D1) *Constructing finite fields.*

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

(b) We will prove in class tomorrow that 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) Recall that 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: this can be done without excessive calculations!

(D2) *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 $\mathbb{F}_q$.

(d) Factor $x^4 - x$ and $x^8 - x$ over $\mathbb{Z}_2$. Hint: look at your answer to problem (D1) 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 $x^q - x$ factors over $\mathbb{Z}_p$.

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

(R1) Fill in the addition and multiplication tables for $\mathbb{F}_8$. Hint: use what we know about finite fields to reduce the number of computations you have to perform.

(R2) Multiply every nonzero element of $\mathbb{F}_5$. Do the same for $\mathbb{F}_{11}$ and $\mathbb{F}_4$.

(R3) Find a formula for the product of all nonzero elements of $\mathbb{F}_{p^r}$. Prove your formula holds.

(R4) For p prime, find the number of irreducible polynomials of degree 2 and 3 in $\mathbb{Z}_p[x]$.

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) Fix a group $(G, +)$ with $n = |G|$. Fix an element $g \in G$, and let m denote the order of g. Let $H = \{ig : 0 \le i < m\}$ (here, ig denotes adding g to itself i times).

(a) Prove that H is closed under addition.

(b) Prove that for all $a \in G$, $a + H = \{a + g^i : 0 \le i < m\}$ has the same size as H.

(c) Fix $a, b \in G$. Prove that if $(a + H) \cap (b + H) \neq \emptyset$, then $a + H = b + H$.

(d) Conclude that m divides n, and in particular that $ng = 0$.

(S2) Fix a prime p.

(a) Argue that $\mathbb{F}_p$ has no proper subfields (that is, a proper subset that is also a field).

(b) Determine the possible sizes of subfields of $\mathbb{F}_{27} = \mathbb{F}_{3^3}$, $\mathbb{F}_{64} = \mathbb{F}_{2^6}$, and $\mathbb{F}_{625} = \mathbb{F}_{5^4}$.

(c) Suppose $\mathbb{F}_{p^t} \subset \mathbb{F}_{p^r}$ for integers $t \le r$. Formulate and prove a conjecture about the relationship between t and r.

You may cite problem (S1) part (d) "free of charge" (i.e. without proof) in your solution.

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) For each prime p, construct a field which has every finite field $\mathbb{F}_{p^r}$ as a subfield. Does there exist a single field that has every finite field as a subfield?