Winter 2017, Math 148: Week 3 Problem Set
Due: Wednesday, February 1st, 2017
Polynomials and Finite Fields

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

(D1) *The polynomial ring* $\mathbb{Z}_n[x]$.

(a) Which elements of $\mathbb{Z}_3[x]$ are units? For which n does this hold?
(b) Can you find a unit in $\mathbb{Z}_4[x]$ with positive degree?
(c) For which n does $\mathbb{Z}_n[x]$ have zero-divisors?
(d) Is it possible to bound the degrees zero-divisors can have in $\mathbb{Z}_6[x]$? How about $\mathbb{Z}_n[x]$?
(e) Which elements of $\mathbb{Z}_4[x]$ are zero-divisors?
(f) Find the common divisor of $2x$ and $4x$ over $\mathbb{Z}_6$ of highest degree.

(D2) *Factoring polynomials over* $\mathbb{Z}_n$.

(a) Factor $x^3 + 3x + 1$ and $x^3 + 3x^2 + 2x + 4$ over $\mathbb{Z}_5$ as a product of irreducibles.
(b) Factor $x^4 + 4$ over $\mathbb{Z}_3$. Does it factor over $\mathbb{Q}$?
(c) Factor $x^5 + 2$ over $\mathbb{Z}_3$. Does it factor over $\mathbb{Q}$?
(d) Find all roots of $3x + 3 = 0$ over $\mathbb{Z}_6$. Why is this surprising?
(e) Find a linear polynomial over $\mathbb{Z}_6$ with no solutions.
(f) Consider the polynomial $f(x) = x^2 - x = (x)(x - 1)$ over $\mathbb{Z}_6$. Find all roots of $f(x)$ and the roots of its factors x and $x - 1$. What do you notice?
(g) Find all factorizations of $f(x) = x^2 - x$ over $\mathbb{Z}_6$.

(D3) *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 characteristic 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 F_6 have characteristic 6?
(f) It turns out that the characteristic of a finite ring must divide the size of the ring. With this in mind, for each possible characteristic of F_6, try writing out the addition and multiplication tables. When are you able to fill both tables?
(g) What can you conclude about F_6?
(h) 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?

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

(R1) Consider the polynomials $f(x) = x^5 + 3x^4 - 7x^3 + 5x + 4$ and $g(x) = 2x^2 + x + 5$. Divide $f(x)$ by $g(x)$ over $\mathbb{Z}_3$. Do the same over $\mathbb{Z}_{11}$. What does this tell you about whether or not $f(x)$ is reducible over $\mathbb{Q}$?

(R2) Find the greatest common divisor of $f(x) = x^6 + x^4 + x^2$ and $g(x) = x^4 + x^3 + x$ over $\mathbb{Z}_3$. Would your answer be different over $\mathbb{Q}$?

(R3) Factor $f(x) = x^5 + 4x^4 + 8x^3 + 11x$ over $\mathbb{Q}$. Hint: first try to factor $f(x)$ over some small finite fields, like $\mathbb{Z}_3$ and $\mathbb{Z}_5$.

(R4) Prove that a finite field must have prime characteristic. You may *not* use the fundamental theorem of finite fields.

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) Consider the set $R = \{a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{R}[x] : a_0 \in \mathbb{Z}\}$ of polynomials over $\mathbb{R}$ with integer constant term.

   (a) Show that R is a ring under the usual addition and multiplication of polynomials.

   (b) Show that some elements of R cannot be factored into a finite product of irreducibles. Hint: consider the element $f(x) = x$.

(S2) Consider the set $R = \{a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{R}[x] : a_1 = 0\}$ of polynomials over $\mathbb{R}$ with no linear term.

   (a) Show that R is a ring under the usual addition and multiplication of polynomials.

   (b) Show that there are elements of R that can be factored in more than one distinct way. Hint: consider the element $f(x) = x^6$.

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) Prove that any finite ring with no zero-divisors is a field.