

Fall 2020, Math 620: Week 11 Problem Set
Due: Thursday, November 12th, 2020
Classifying Finite Fields

Discussion problems. The problems below should be worked on in class.

- (D1) *Finite fields.* The goal of this problem is to systematically build “small” finite fields.
- (a) Fill in the operation tables of a field $F_4 = \{0, 1, a, b\}$ with exactly 4 elements.
 - (b) What familiar additive group did you obtain for $(F_4, +)$? With this in mind, is the multiplication structure what you expected it to be?
 - (c) Let’s attempt to do the same for a field F_6 with exactly 6 elements. Hint: what can its characteristic be? Use the characteristic to give convenient names to some of the elements, and to fill in part of the table.
 - (d) Fill in the addition and multiplication tables for a 5-element field $F_5 = \{0, 1, a, b, c\}$ (this is tricky, but a fun challenge!). How many are there (up to isomorphism)?
- (D2) *Constructing finite fields.* The fields constructed in this problem will be used in (D3). Note: use “ z ” instead of “ x ” as your variable throughout this problem!
- (a) For each prime p , locate a field \mathbb{F}_p with exactly p elements.
 - (b) Locate an ideal $I = \langle f(z) \rangle \subset \mathbb{Z}_2[z]$ so that $\mathbb{F}_4 = \mathbb{Z}_2[z]/I$ is a field with 4 elements. Hint: what must $\deg f(z)$ be? Since $f(z) \in \mathbb{Z}_2[z]$, how many polynomials are there of that degree?
 - (c) Using this idea, construct fields \mathbb{F}_8 and \mathbb{F}_9 with 8 and 9 elements, respectively.
 - (d) Construct a field \mathbb{F}_{16} with 16 elements. Why is this (slightly) more tricky?
- (D3) *Factoring polynomials over finite fields.* For clarity in this problem, use “ z ” when writing elements of each finite field \mathbb{F}_q constructed above, and use “ x ” as the variable in $\mathbb{F}_q[x]$. You may omit the brackets for elements of \mathbb{F}_q , for instance, $\mathbb{F}_4 = \{0, 1, z, z + 1\}$.
- (a) Factor the polynomial $x^5 - x$ over \mathbb{F}_5 . Do the same for $x^7 - x$ over \mathbb{F}_7 . Hint: for both, begin by looking for roots.
 - (b) Factor the polynomial $x^4 - x$ over \mathbb{F}_4 (here, you may use z and $z + 1$ as **coefficients** when you factor).
 - (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 .
 - (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 $x^{p^r} - x$ factors over \mathbb{Z}_p (proof not required!).
 - (g) Factor $x^{16} - x$ over \mathbb{F}_4 . Does this hint at an extension of your conjecture from part (f)?

Homework problems. You must submit *all* homework problems in order to receive full credit.

- (H1) Factor $f(x) = x^5 + x^4 + 1$ over \mathbb{F}_2 , \mathbb{F}_4 , and \mathbb{F}_8 .
- (H2) Determine how many elements of \mathbb{F}_{32} are primitive. Hint: no excessive calculations needed!
- (H3) Find a formula for the product of all nonzero elements of \mathbb{F}_q .
- (H4) (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.
- (H5) Determine whether each of the following statements is true or false. Prove your assertions.
- (a) No finite field is algebraically closed (recall that a field F is *algebraically closed* if every polynomial in $F[x]$ has a root in F).
- (b) The finite field \mathbb{F}_{p^r} has a subfield (that is, a subring that is also a field) with exactly q elements if and only if $q = p^t$ for some $t \leq r$.

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) Fix a finite field \mathbb{F}_q , and let $a(n)$ denote the number of irreducible polynomials over \mathbb{F}_q of degree exactly n . Prove that

$$\lim_{n \rightarrow \infty} \frac{a(n)}{q^n} = 0,$$

meaning that irreducible polynomials are “sparse” in $\mathbb{F}_q[x]$.