Suggested reading: handout on Field Axioms; Trappe-Washington 3.11, 16.1–3.

1. For this question, refer to your handout on Field Axioms.
   (a) State which of the examples in Section 2 are fields, and for each of the non-fields, cite at least one axiom that fails. No proof needed.
   (b) Using the definition of a multiplicative inverse, prove that for any nonzero $a \in \mathbb{F}$, $(a^{-1})^{-1} = a$.
   (c) Using the field axioms, prove that $a \cdot 0 = 0$ for any $a \in \mathbb{F}$. *Hint*: Expand $a \cdot (1 + 0)$ in two ways.
   (d) Using the field axioms and Part (b), prove that fields have no (nonzero) zero divisors.
   (e) Let $\mathbb{F}$ be a finite field with multiplicative identity 1. We define the *characteristic* of $\mathbb{F}$ to be the smallest positive number n such that the sum
   $$\underbrace{1 + 1 + \cdots + 1}_{n \text{ times}}$$
   is equal to the additive identity zero. Prove that, if $\mathbb{F}$ is finite, then it has a finite characteristic n. Further prove that the characteristic of $\mathbb{F}$ must be prime.

   Note: For some infinite fields, such as $\mathbb{Q}$ and $\mathbb{R}$, the sum of any number of 1's is nonzero. These fields are said to have *characteristic zero*.
   Note: For a field $\mathbb{F}$, it is standard to refer to the sum
   $$\underbrace{1 + 1 + \cdots + 1}_{n \text{ times}}$$
   by the number n. With this convention, we can identify a copy of the integers $\mathbb{Z}$ in any field of characteristic zero, and a copy of the field $\mathbb{Z}/p\mathbb{Z}$ in any field of characteristic p.

2. Let $\mathbb{F}_p$ denote the field $\mathbb{Z}/p\mathbb{Z}$ for some positive prime p. Let $\mathbb{F}_p[x]$ denote the set of polynomials in the variable x with coefficients in $\mathbb{F}_p$.
   (a) What is an *irreducible* polynomial $P(x)$? Show by example that polynomials that are irreducible over the integers may not be irreducible over $\mathbb{F}_p[x]$, and that polynomials that are irreducible over $\mathbb{F}_p[x]$ may not be irreducible over $\mathbb{F}_q[x]$ for $q \neq p$.
   (b) Let $P(x) \in \mathbb{F}_p[x]$ be a polynomial of degree d. Define the *congruence classes* of $\mathbb{F}_p[x]$ modulo $P(x)$, and compute how many congruence classes there are.
   (c) Explain how to construct a finite field with p^k elements (Chapter 3.11).
   (d) Explain why the object you've constructed is a field. Specifically, explain why the one non-obvious field axiom holds: nonzero elements have multiplicative inverses.
   (e) Remark that every polynomial in $P(x) \in \mathbb{F}_p[x]$ defines a *polynomial function* on $\mathbb{F}_p$, mapping $b \in \mathbb{F}_p$ to the congruence class $P(b) \in \mathbb{F}_p$ obtained by substituting $x = b$. Give an example of how two different polynomials can define the same function on $\mathbb{F}_p$ (*Hint*: If $a \in \mathbb{F}_p$, what is $a^p \pmod p$?) Note that the two polynomials in your example are still considered distinct elements in $\mathbb{F}_p[x]$, even if they define the same function $\mathbb{F}_p \to \mathbb{F}_p$.

3. (a) Determine all irreducible polynomials in $\mathbb{F}_3[x]$ of degree 2 or less.
   (b) Write down the addition and multiplication table for $\mathbb{F}_2[x]$ modulo $(x^2 + x + 1)$.
   (c) The polynomials $P(x) = 1 + x + x^3$ and $Q(x) = 1 + x^2 + x^3$ are both irreducible in $\mathbb{F}_2[x]$. Since both have degree 3, we can identify the congruence classes of $\mathbb{F}_2[x]$ modulo $P(x)$ and the congruence classes of $\mathbb{F}_2[x]$ modulo $Q(x)$ with the eight polynomials $\mathbb{F}_2[x]$ of degree 2 or less (all possible remainders on division by a degree 3 polynomial). Show by example that the addition and multiplication rules for these small-degree polynomials are different in $\mathbb{F}_2[x]$ modulo $P(x)$ and $\mathbb{F}_2[x]$ modulo $Q(x)$. This is one reason it should be surprising that these two fields (and any two finite fields with the same number of elements) are "isomorphic", possibly after re-labeling the elements.

(d) Use the Euclidean algorithm (and polynomial division) to find a multiplicative inverse for $x+1 \pmod{x^3+x^2+1}$ in $\mathbb{F}_2[x]$.

4. Let E be an elliptic curve defined over a field K. As usual, assume that 2 and 3 have multiplicative inverses in K.
   (a) Explain why the addition law is *commutative*, that is, why $P+Q=Q+P$ for any points P, Q.
   (b) Explain what it means to say that the addition law is *associative*. (This result is onerous to prove, and we will omit the proof.)
   (c) Given a point $P \neq \infty$ on an elliptic curve, what is its negative $(-P)$? Use the equation for E to explain why $-P$ will always be a point on the elliptic curve (that is, why the curve must have reflectional symmetry in the x-axis).
   (d) Give an algebraic description of the addition law (as on Page 362).
   (e) Suppose that P and Q are two distinct points on an elliptic curve not equal to ∞. Let the line through P and Q intersect the curve in a third point R. Verify that the coordinates of $P+Q$, defined to be the reflection over the x-axis of R, are given by the formula you wrote down in the previous part. You may assume that $K=\mathbb{R}$ so you are comfortable with the geometry, but your solution (plus knowledge of algebraic geometry) will work in general.
5. Trappe–Washington Chapter 16 Exercise 2.
6. Trappe–Washington Chapter 16 Exercise 4.
7. Trappe–Washington Chapter 16 Exercise 15.

The following two bonus questions (which are very challenging) together prove our claim that every finite field can be realized by the construction described in Chapter 3.11.

8. **Bonus.** Prove that the number of elements in any finite field must be a prime power.
9. **Bonus.** Prove that any two finite fields with the same number of elements are isomorphic.

The following questions give applications of elliptic curves to cryptography.

10. **Bonus**.
    (a) Let $n=pq$. Explain how we can factor n by analyzing elliptic curves over $\mathbb{Z}/n\mathbb{Z}$.
    (b) Trappe–Washington Chapter 16 Exercise 6(a).
11. **Bonus.** Trappe-Washington Chapter 16 Exercise 9.