1 Textbook problems

We will not be releasing solutions for the textbook problems. If you would like to see a solution to a specific problem, feel free to ask during office hours.

2 Finite fields revisited

1. Denote \( \pi = \prod_{k=1}^{n} (k+1) \), where 1 is the multiplicative identity in \( k \). Suppose \( c_k \) is not prime. Then there exist positive integers \( m, n \) such that \( 1 < m, n < c_k \) and \( c_k = mn \). Then observe that

\[
\pi \cdot \pi = c_k = 0
\]

in \( k \). Observe that since \( 1 < m < c_k \), by definition of \( c_k \), \( \pi \neq 0 \). Since \( k \) is a field, \( \pi \) must have a multiplicative inverse; call its multiplicative inverse \( x \). Multiplying both sides of equation (1) by \( x \) yields

\[
x \cdot \pi \cdot \pi = x \cdot 0 \implies \pi = 0.
\]

But \( 1 < n < c_k \), contradicting the definition of \( c_k \). It follows that \( c_k \) cannot be composite and is therefore prime.

2. Vector addition is taken care for free; to add two vectors, we can just compute their sum in \( k \). We just need to define scalar multiplication by an element of \( \mathbb{F}_p \). Given \( c \in \mathbb{F}_p = \{0, 1, \ldots, p-1\} \), for \( v \in k \) we can define \( c \cdot v = \pi \cdot v \) where the multiplication is computed in \( k \). It is straightforward to check that this definition satisfies the required properties. The only slightly tricky point is associativity. Let \( a, b \in \{0, 1, \ldots, p-1\} \) and let \( c = ab \) in \( \mathbb{F}_p \) with \( c \in \{0, 1, \ldots, p-1\} \). (Note in particular that we do not necessarily have \( ab = c \) as integers. For instance, if \( p = 5 \) and we take \( a = b = 4 \), then \( ab = 16 \) but \( c = 1 \).) We have \( (a \cdot b) \cdot v = \pi \cdot v \). On the other hand, \( a \cdot (b \cdot v) = \pi \cdot \pi \cdot v = \pi^2 \cdot v \). However, since \( \pi = 0 \) in \( k \) and \( ab \equiv c \) (mod \( p \)), we can subtract multiples of \( p \)s from \( \pi \) to reduce it to \( \pi \) without changing the value in \( k \). So these two values actually agree and our definition of scalar multiplication is indeed associative.

3. We know that \( k \) must be finite dimensional. This is because \( k \) has a finite spanning set, namely itself (\( k \) is finite). Let \( \dim_{\mathbb{F}_p}(k) = n \) and let \( v_1, v_2, \ldots, v_n \) be a basis for \( k \) over \( \mathbb{F}_p \). Note that for each choice of \( a_1, \ldots, a_n \in \mathbb{F}_p \), we have a unique element \( a_1v_1 + \cdots + a_nv_n \in k \), and furthermore every element of \( k \) has a unique representation in this form. Thus there is a bijection between elements of \( k \) and \( n \)-tuples \( (a_1, \ldots, a_n) \) of elements of \( \mathbb{F}_p \). Since there are \( p \) choices for each of the \( n \) coefficients \( a_i \), there are \( p^n \) such tuples and therefore exactly \( p^n \) elements in \( k \), i.e. \( |k| = p^n \) as desired.
4. We have $4 = 2^2$ so we will want to think of our field $k$ as a vector space over $\mathbb{F}_2$. Note that for any element $x \in k$, we have

$$x + x = 1 \cdot x + 1 \cdot x = (1 + 1) \cdot x = 0 \cdot x = 0,$$

so every element must be its own multiplicative inverse. Using this information, we can systematically define the rest of the structure in $k$.

We know that $k$ contains two elements 0 and 1 with $0 \neq 1$ (the standard additive and multiplicative identities). We can’t generate any new elements simply by adding or multiplying these with each other, so let us simply name another element $a \neq 0, 1$. Observe that $a + 1 \neq 0, 1, a$. If $a + 1 = 0$ then adding 1 to both sides shows us $a = 1$, a contradiction. The other two cases can be dealt with similarly, so we see that $a + 1$ must be the fourth element of the field. Addition is completely specified by the fact that $x + x = 0$ for all $x$ (and the fact that addition is commutative and associative), so we just need to define the multiplicative structure of the field.

Since we want multiplication to distribute over addition, we note that we need $a(a + 1) = a^2 + a$ and $(a + 1)^2 = a^2 + 2a + 1 = a^2 + 1$, so we can completely specify multiplication by saying what the value of $a^2$ is. We know $a^2 \neq 0$ since nonzero elements cannot multiply to 0 in a field. If $a^2 = 1$ then $(a + 1)^2 = a^2 + 1 = 1 + 1 = 0$, contradicting the fact that $a + 1 \neq 0$. If $a^2 = a$ then multiplying by the multiplicative inverse of $a$ on both sides (which must exist since $a \neq 0$) gives us $a = 1$. The only choice left to us is then $a^2 = a + 1$. This completely specifies the additive and multiplicative structure of $k$, and it is straightforward to check that $k$ satisfies all of the field axioms (in particular existence of multiplicative inverses). So $k$ is a field with 4 elements.