1 Constructing the rational numbers
   
i) We will construct $\mathbb{Q}$ as a set using an equivalence relation on $\mathbb{Z} \times (\mathbb{Z} - \{0\})$. Namely, let $(a, b) \sim (c, d)$ if and only if $ad = bc$. Then define $\mathbb{Q} := (\mathbb{Z} \times (\mathbb{Z} - \{0\}) / \sim$. It is customary to denote an element $(a, b)$ of $\mathbb{Z} \times (\mathbb{Z} - \{0\})$ by $\frac{a}{b}$. Make sure you understand why. Where does this equivalence relation come from?

ii) Define the field operations $+$ and $\cdot$ on $\mathbb{Q}$ as they should be using the intuition you have. Check that these definitions indeed make $\mathbb{Q}$ a field.

2 Finite fields
   
Let $k$ be a finite field.

i) Prove that there must exist a positive integer $n$ such that $\underbrace{1 + 1 + \cdots + 1}_{n \text{ times}} = 0$. Define $c_k$ to be the smallest such $n$.

ii) Prove that $c_k$ must divide $|k|$, the number of elements in $k$. Feel free to look up Lagrange’s theorem and use it (without proving) for this problem. Everything else, including the fact that the theorem applies, needs to be proven of course.

iii) Now assume that $|k| = p$, where $p$ is a prime number. Prove that $c_k = p$.

iv) Prove that there exists exactly one field with $p$ elements.
   
   (Hint: To do this, first show that at least one field with $p$ elements exists. We have already constructed two operations on a set of $p$ elements in class. You only need to check that the field axioms are satisfied. Secondly, you will need to show that this is the only field with $p$ elements. For this part, start by representing the elements of the field as $1 + 1 + \cdots + 1$)
3 Subfields

i) Let $k$ be a field and $F \subset k$ be a subset. Assume that:

- $0, 1 \in F$.
- If $a \in F$, then $-a \in F$.
- If $a \in F \setminus \{0\}$, then $a^{-1} \in F$.
- If $a, b \in F$, then $a + b \in F$.
- If $a, b \in F$, then $a \cdot b \in F$.

Prove that if one endows $F$ with the same operations as $k$, then $F$ is itself a field. We call $F$ a subfield of $k$.

ii) Inside $\mathbb{C}$, we have the set of purely real numbers:

$$A := \{a + i \cdot 0 \mid a \in \mathbb{R}\} \subset \mathbb{C}.$$ 

We also have the set of purely imaginary numbers:

$$B := \{0 + i \cdot b \mid b \in \mathbb{R}\} \subset \mathbb{C}.$$ 

Which of $A$ and $B$ are subfields of $\mathbb{C}$?

4 Solving an equation over different fields

For which of the following fields does the equation $x^2 + 2x + 2 = 0$ have a solution? $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{F}_p$ with $p$ prime
(Note: By $x^2$ we mean $x \cdot x$, and by 2 we mean $1 + 1$ where 1 is the multiplicative identity in whichever field we are considering.)

Added on Jan 17: You can use the following fact without proof. For every prime $p$, there exists an element $g$ in $\mathbb{F}_p$ such that the smallest positive integer $k$ so that $g^k = 1$ is $k = p - 1$. 

2