Since we’re studying finite combinatorial structures, we’ll have to do algebra and linear algebra over finite fields. The most familiar of these are the prime fields $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ where $p \in \mathbb{Z}$ is a prime. In general any finite field $F$ contains a unique prime field, consisting of all the elements of $F$ of the form $1 + 1 + \ldots + 1$. The size, call it again $p$, of this prime field is the characteristic of $F$. Since $F$ is a vector space over $\mathbb{F}_p$, we have $#F = p^n$ for some natural number $n$ (namely the dimension of that vector space). We cite without proof the following fundamental theorem, due in essence to Galois:

For each prime $p$ and integer $n \geq 1$ there exists a finite field $F$ of cardinality $p^n$. This field is unique up to isomorphism. The automorphism group of $F$ is canonically isomorphic with $\mathbb{Z}/n\mathbb{Z}$ and is generated by the Frobenius automorphism $x \mapsto x^p$. For each positive divisor $m$ of $n$, that field contains a unique subfield $F_1$ of cardinality $q^m$, namely $\{x : x^{q^m} = x\}$. The field extension $F/F_1$ is normal, with cyclic Galois group of order $m/n$ generated by $x \mapsto x^{p^m}$.

We shall use $\mathbb{F}_q$ for the finite field of cardinality $q = p^n$; the older notation $\text{GF}(q)$ for $\mathbb{F}_q$ (“GF” as in “Galois field”) is still occasionally seen in the literature. These fields are a natural and important generalization of the familiar prime fields $\mathbb{F}_p$; in general anything that can be done with $\mathbb{F}_p$ works just as well with $\mathbb{F}_q$, and sometimes one can do a bit more with the non-prime fields thanks to the nontrivial automorphisms (as is true for $\mathbb{C}$, which though less familiar than $\mathbb{R}$ turns out to be equally fundamental and sometimes more tractable). For example, you probably know that for every prime $p$ there is at least one “primitive residue” mod $p$, which is to say that the multiplicative group $\mathbb{F}_p^\ast$ is cyclic; the same is true (with much the same proof) for $\mathbb{F}_q^\ast$ for any finite field $\mathbb{F}_q$. Warning: once $n > 1$, the finite field of $p^n$ elements is not $\mathbb{Z}/p^n\mathbb{Z}$ (and its additive group is not cyclic).

Except for the familiar prime fields (with $n=1$), the only finite fields we shall have much use for are $\mathbb{F}_4$ and $\mathbb{F}_9$; these may be defined as the quadratic extensions $\mathbb{F}_2(\rho)$ and $\mathbb{F}_3(i)$ of their prime fields, where $\rho^2 + \rho = 1$ and $i$ is a square root of $-1$. 