Set 7

(A) More on induction

(1) Consider the following argument using mathematical induction. Is it correct?

Theorem. *In any group of finitely many people, any two people have the same eye color.*

Proof. We prove this by induction, showing that for any $n \geq 1$, in any group of n people, everyone has the same eye color. The base case $n = 1$ is clearly true. Suppose then that the statement is true for any group of n people. We must show it is true for any group of $n + 1$ people. For convenience, let us label the members of our group of $(n + 1)$ people as $A_1, A_2, \ldots, A_{n+1}$. Consider the groups of n people $\{A_1, A_2, \ldots, A_n\}$ and $\{A_2, A_3, \ldots, A_{n+1}\}$. By the induction assumption (that the statement is true for groups of n people), persons $A_1, A_2, \ldots, A_n$ all have the same eye color; and similarly persons $A_2, A_3, \ldots, A_{n+1}$ all have the same eye color. Since there is a person (e.g. A_2) belonging to both groups, in fact everyone in both groups must have the same eye color. $\square$

(2) Let f_n denote the n-th Fibonacci number. Show that $f_n \leq 2^n$ for every n. You may need to use strong induction.

(3) Our next goal is to prove the fundamental theorem of arithmetic, given below.

Theorem 4. *Every integer $a > 1$ can be represented as a product of primes $a = p_1^{e_1} p_2^{e_2} \cdots p_s^{e_s}$, where $p_1 < p_2 < \cdots < p_s$, and this representation is unique.*

(i) Start by showing that, if p is a prime number and a, b are integers such that $p|ab$, then $p|a$ or $p|b$. [Hint: translate this to a statement about $\mathbb{Z}/p$, and use that $\mathbb{Z}/p$ is a field.]

(ii) Now prove the fundamental theorem of arithmetic by using strong induction.

(B) The primitive root theorem:

Our goal here is to understand and prove the following result, which we conjectured last week.

Theorem 5. *Let p be a prime number. Then there is a unit u in $\mathbb{Z}/p$ with order $p - 1$.*

Recall that everything in $\mathbb{Z}/p$ is a unit except 0.

(1) For a nonzero element $u \in \mathbb{Z}/p$, show that u has order $p - 1$ if and only if $(\mathbb{Z}/p)^\times = H_u$, using the notation of part (B). This means that every element of $(\mathbb{Z}/p)^\times$ can be written as a power of u. Groups with this property are called *cyclic groups*, and hence Theorem 5 can be rephrased as "The group $(\mathbb{Z}/p)^\times$ is cyclic".

For the next problem, we will assume the following lemma[1], which we will prove later:

Lemma. *Let A be a finite abelian group. Suppose $a \in A$ has order m and $b \in A$ has order k. Then there is an element of A that has order* $\mathrm{lcm}(m, k)$.

(2) Since $(\mathbb{Z}/p)^\times$ is a finite group, amongst all the orders of all its elements there must be a maximal one. Call this maximal order m, and choose $u \in (\mathbb{Z}/p)^\times$ with order m (note: there may be more than one u with this property!). Show that the order of every $v \in (\mathbb{Z}/p)^\times$ must divide m. [Hint: argue by contradiction: suppose $v \in (\mathbb{Z}/p)^\times$ has order k, where k does not divide m. Then use the lemma.]

(3) Show that every element of $(\mathbb{Z}/p)^\times$ is a root of the polynomial $x^m - 1$, and use this to argue that $m \geq p - 1$.

(4) Finish the proof of Theorem 5.

[1] A lemma is a fact that, although perhaps not very interesting by itself, can be used to prove a deeper result

(C) Proof of the Lemma: The following chain of exercises proves the lemma. We will take A to be an abelian group, which we will write additively (this means that the operation in our group is "+" instead of "·", and our identity element is written as "0"). Given an integer $n > 0$ and an element $a \in A$, we will write na for $na = a + a + \cdots + a$ (n times), and when $n < 0$ the element na will mean $na = (-a) + (-a) + \cdots + (-a)$ (n times). Note that the order of a is the smallest integer $n > 0$ for which $na = 0$.

(1) We will first assume that m and k are relatively prime, so that $\operatorname{lcm}(m, k) = mk$. In this case, we will show that the element $u + v$ has order mk. We begin by letting t be the order of $u + v$. Show that $km(u + v) = 0$, and thus t divides km.

(2) Use the fact that $t(u + v) = 0$ to show that the order of tu is equal to the order of tv.

(3) On the other hand, show that the order of tu is $\operatorname{lcm}(m, t)/t$ and that the order of tv is $\operatorname{lcm}(k, t)/t$.

(4) Show that, for any two positive integers r and s, we have $\operatorname{lcm}(r, s) = rs/\gcd(r, s)$. Use this to conclude that, in the context of our problem, we have

$$m \gcd(k, t) = k \gcd(m, t).$$

(5) Finish the proof of the lemma in the case that $\gcd(m, k) = 1$. [Hint: if $\gcd(m, k) = 1$, and m divides ks, then m must divide s.]

(6) Proof the general result. [Hint: let $u' = \gcd(m, k)u$. Show that the order of u' is $m/\gcd(m, k)$, and hence u' and v have coprime orders, so we can apply the lemma to the pair (u', v). Part (4) might also be useful.]