Prove Lagrange's theorem for orders in the special case that G is a finite abelian group.

Let $G = \{g_1, g_2, g_3, \ldots, g_n\}$ and Let $g \in G$. Let $h = g_1 g_2 g_3 \ldots g_n$ The map $x \mapsto gx$ is a bijection, so $h = gg_1 gg_2 gg_3 \ldots gg_n$ for some permutation of g_i. However, because G is abelian h is the same no matter the permutation. Then, we can simplify this to $h = g^n h$ therefore g^n is the identity.

Let p be a prime. Show that the only group of order p is Z/pZ.

Let G be a group with order p. Let 0 be the identity element. p is prime, so $p \geq 2$, which means there must be at least one other element g which is not the identity element. Let H be the subgroup generated by g. If $|H| = |G|$, then we are done through the map $n \mapsto g^n$.

Assume then that $|H| \neq |G|$. $|H|$ has to be smaller than $|G|$, because otherwise G is not closed. By lagrange's theorem, $g^{|H|} = 0$, and $g^{|G|} = 0$, so $g^{k|H| \mod |G|} = 0$, for $k \in \mathbb{N}$

$(Z/pZ)^\times$ is a group with size $p-1$, so therefore by Lagrange's theorem, for any $x \in (Z/pZ)^\times$,

$$x^{p-1} = 1 \pmod p \tag{1}$$

Equation 1 is fermat's little theorem. Since we know $|G|$ is prime, by Fermat's Little theorem, $|H|^{|G|-1} \mod |G| = 1$,

so $g = 0$, but we said that g was not the identity, so $|H| = |G|$, and they are isomorphic.

Let p be a prime and $F_1 = F_2 = 1, F_{n+2} = F_{n+1} + F_n$ be the Fibonacci sequence. Show that $F_{2p(p^2-1)}$ is divisible by p.

We can turn the fibonacci sequence into a matrix using

$$g = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$$

because

$$\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^n = \begin{pmatrix} F_{n+1} & F_n \\ F_n & F_{n-1} \end{pmatrix}$$

This is proved using induction. The base case is $n = 1$ and is true, then

$$g^{n+1} = gg^n = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} F_{n+1} & F_n \\ F_n & F_{n-1} \end{pmatrix} = \begin{pmatrix} F_{n+2} & F_{n+1} \\ F_{n+1} & F_n \end{pmatrix}$$

If the field of the matrix is $\mathbb{Z}/p\mathbb{Z}$, and we prove that $g^n = I$, where I is the identity matrix, then we will have shown that $F_n = 0 \mod p$.

Observe that the determinant of g is -1. Note that the set of all 2 by 2 matrices mod p with determinant ± 1 forms a group. It has an identity element, matrix multiplication is associative, and the inverse of each matrix also has the determinant ± 1.

Let this group be G. Then all elements of this group are forms of $ad - bc = \pm 1$, a, b, c, d greater than equal 0 and less than p. If we can show that $|G| = 2p(p^2 - 1)$, then by Lagrange's theorem, $g^{|G|} = I$,completing the proof.

For now consider forms of $ad - bc = 1$ For any value ad, there exists a unique value that bc must be to satisfy the equation.

Split this into cases where $ad = 1$ and $ad \neq 1$

case 1 If $ad = 1 \mod p$, then both a and d canot be 0, and if a is non zero then there is a unique vaule that d must be, so there are $p - 1$ pairs of a, d that satisfy $ad = 1 \mod p$. Then $bc = 0 \mod p$, so b or c must be 0, so there are $2p - 1$ pairs of b, c, that satisfy this. Therefore, there are $(p - 1)(2p - 1)$ total.

case 2: If $ad \neq 1$, then of the p^2 total pairs of a, d, we subtract those that have $ad = 1$, leaving us with $p^2 - p + 1$ pairs. By the same reason that there are $p - 1$ pairs that satisfy $ad = 1$, there are $p - 1$ pairs of b, c that wil satisfy $bc = 1 - ad$, leaving $(p^2 - p + 1)(p - 1)$ total.

Combining the cases, we get $(p - 1)(p^2 + p)$ matrices that have determinant 1. By a similar proof, we can show there are $(p - 1)(p^2 + p)$ matrices that have determinant -1. In total there are $2(p - 1)(p^2 + p) = 2p(p^2 - 1)$, so $|G| = 2p(p^2 - 1)$, which completes the proof.