MAT347 TUTORIAL 3

For n a positive integer let $\phi(n)$ be the number of positive integers less than n that are coprime to n (the **Euler totient** function).

(1) Prove that the number of generators of $\mathbb{Z}/n\mathbb{Z}$ is equal to $\phi(n)$.
(2) Use the previous problem to prove that $n = \sum_{d|n} \phi(d)$, where $d|n$ means d is a divisor of n. (Hint: start with Lagrange's theorem).

Suppose G is a finite group of order n. Let G_d be those elements of G with order d and let G^d be those elements whose order divides d.

(3) Prove that $G_d = \emptyset$ if d does not divide n.
(4) Suppose that for some d, $\left|G^d\right| \leq d$. Prove that $G_d = \emptyset$ or else G^d is a cyclic subgroup and $|G_d| = \phi(d)$.
(5) Suppose that for all d, $\left|G^d\right| \leq d$. Prove that G is cyclic. (Hint: show that $G_d \neq \emptyset$ for any d dividing n and then take $d = n$)
(6) Suppose $\mathbb{F}$ is a field. Let $\mathbb{F}^x$ denote its *group of units*, i.e. the set $\mathbb{F}^x = \mathbb{F} \setminus \{0\}$ with group operation multiplication. Use (without proof) the fact that over any field, a degree d polynomial has at most d roots to prove that any finite subgroup of $\mathbb{F}^x$ is cyclic. (Hint: use the previous problem).
(7) Conclude that $(\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic for any prime p.