Mathematics 4340
When are all groups of order n cyclic?
Ken Brown, Cornell University, March 2009

Additional problem 2 on Assignment 8 characterizes the integers n such that every group of order n is cyclic. This handout gives the complete solution.

Theorem. *Let S be the set of integers whose prime factorization has the following two properties:*

(i) No prime occurs more than once.

(ii) There is no pair of primes p, q with $p \mid (q-1)$.

Then S is precisely the set of integers n such that every group of order n is cyclic.

Proof. We begin with the easier part, which is that if $n \notin S$, then there is a noncyclic group of order n. If (i) fails, then n factors as p^2m for some prime p. Then $\mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_m$ is a noncyclic group of order n [because it has the noncyclic subgroup $\mathbb{Z}_p \times \mathbb{Z}_p$]. If (ii) fails, then n factors as pqm, where p and q are primes such that $p \mid (q-1)$. Since $\mathrm{Aut}(\mathbb{Z}_q)$ is cyclic of order $q-1$, we can form a semidirect product $H := \mathbb{Z}_q \rtimes \mathbb{Z}_p$ with a nontrivial action of $\mathbb{Z}_p$ on $\mathbb{Z}_q$. Then $H \times \mathbb{Z}_m$ is a noncyclic (even nonabelian) group of order n.

Turning now to the harder part, we must show that if G is a finite group whose order is in S, then G is cyclic. Arguing by induction on $|G|$, we may assume that every proper subgroup of G is cyclic and every proper quotient of G is cyclic. In particular, every proper subgroup is abelian, so G is not a nonabelian simple group. (See the handout "A nonabelian finite simple group has a proper nonabelian subgroup".) And we may assume that G is not an abelian simple group either, since then it would trivially be cyclic. So G has a proper, nontrivial normal subgroup N, which is cyclic by the induction hypothesis, and the quotient G/N is cyclic for the same reason.

I claim that N has a complement. Write $|G| = ab$, where $a := |N|$ and $b := |G/N|$. Since a and b are relatively prime by condition (i), the claim will follow by a counting argument if we show that G has a subgroup of order b. Start with $H := \langle x \rangle$, where $x \in G$ is chosen so that its image in G/N generates the latter. Then H surjects onto G/N, so its order is divisible by b. But now a known result about cyclic groups implies that H has a subgroup Q of order b, and the claim is proved.

We now have $G \cong N \rtimes Q \cong \mathbb{Z}_a \rtimes \mathbb{Z}_b$, and we will be done if we can show that $\mathbb{Z}_b$ necessarily acts trivially on $\mathbb{Z}_a$. Recall that there is a ring isomorphism $\mathbb{Z}_a \cong \prod_q \mathbb{Z}_q$, where q ranges over the primes dividing a; hence

$$\mathrm{Aut}(\mathbb{Z}_a) \cong \mathbb{Z}_a^\times \cong \prod_q \mathbb{Z}_q^\times.$$

In particular, $|\mathrm{Aut}(\mathbb{Z}_a)| = \prod_q (q-1)$. Condition (ii) now implies that b is relatively prime to the order of $\mathrm{Aut}(\mathbb{Z}_a)$, so the action of $\mathbb{Z}_b$ on $\mathbb{Z}_a$ is indeed trivial $\square$