Math 300— Homework Set 5

Due Thursday, March 27

1. Read chapters 5.1, 5.2, and 5.4 in the book (and skim 5.3)
2. In chapter 3: 67
3. In chapter 5: 2, 5, 6, 36, 37
4. Fix a number a and a prime number p where $p \not| a$. We know that $a^{p-1} \equiv 1 \mod p$ by Fermat's Little Theorem. Considering all the positive integers k for which $a^k \equiv 1 \mod p$, let r be the smallest one. We know that r exists by the well-ordering principle. To be explicit, r is the minimal element in the non-empty set:
$$\{k \in \mathbb{N} \mid a^k \equiv 1 \mod p\}.$$
Show that $r|(p-1)$.
5. For $p = 13$ and each $a \in \{1, 2, 3, \ldots, 11, 12\}$, find the smallest positive integer r for which $a^r \equiv 1 \mod p$.