Abstract Algebra - Worksheet 8

Here is a theorem of elementary number theory, which we have been using, and will continue to use, without proof:

The division algorithm. Suppose n and m are integers, with $m > 0$. Then there exist *unique* integers q and r with $n = mq + r$, and $0 \leq r < m$.

1. Suppose that G is a group, and $a \in G$. Prove that if the order of a is m, then for all integers q and r, $a^{mq+r} = a^r$.
2. Prove that every cyclic group is abelian.
3. Prove that if $G \times H$ is a cyclic group, then G and H are cyclic groups.
4. Prove or disprove, as appropriate: If G and H are cyclic groups, then $G \times H$ is a cyclic group.
5. Suppose H is a subgroup of a group G with $a \in G$. Suppose n, m, q and r are integers with $n = mq + r$. Prove that if a^n and a^m are both in H, then so is a^r.

The following is usually taken as an axiom when working with non-negative integers, and we will do the same:

Well-ordering principle: Every non-empty set of positive integers contains a least element.

6. Suppose that G is a cyclic group, with generator a. Prove that if H is a subgroup of G then H is cyclic.
7. Suppose n and m are integers. Let $H = \{sm + tn \mid s \in \mathbb{Z} \text{ and } t \in \mathbb{Z}\}$. Prove that H is a cyclic subgroup of $\mathbb{Z}$.
8. Suppose n and m are integers. In the previous problem we showed that $H = \{sm+tn \mid s \in \mathbb{Z} \text{ and } t \in \mathbb{Z}\}$ is a cyclic subgroup of $\mathbb{Z}$. Prove that if d is a generator of H, then $d = \gcd(m, n)$.
9. Suppose n and m are integers, with $d = \gcd(m, n)$. Prove that there exist integers s and t with $sm + tn = d$.