Several facts regarding $U(n)$

Math 307 - Spring 2012

In class, we defined the group $U(n)$. The definition of $U(n)$ was based on a Homework problem in a crucial way. Here is the problem, and its solution:

Problem. Let a and n be positive integers, and let $d = \gcd(a, n)$. Prove that $ax \equiv 1(\text{mod } n)$ has a solution if and only if $d = 1$.

Solution. First, assume that $d = 1$. Then, by the Corollary to Theorem 0.2 in the text, which we proved in class, there exist integers s and t such that $as + nt = 1$. We may rewrite this equation as $as - 1 = (-t)n$, which means that n divides $as - 1$. This implies (by definition, or by the book's definition and by Exercise 9 on pg. 22,) that $as \equiv 1(\text{mod } n)$. Therefore, we have $x = s$ is a solution to $ax \equiv 1(\text{mod } n)$.

Conversely, suppose that there is some solution x satisfying $ax \equiv 1(\text{mod } n)$. Then n divides $ax - 1$, and so there is an integer q such that $ax - 1 = qn$. We may rewrite this equation as $ax + n(-q) = 1$, where x and $-q$ are integers. By the last statement of Theorem 0.2 in the text, we know that d is the smallest positive integer which is in the form $as + nt$ for $s, t \in \mathbb{Z}$. Since we now have 1 in this form, and 1 is the smallest positive integer, then we must have $d = 1$. $\square$

In class, we defined $U(n)$ to be the set of positive integers less than n which are relatively prime to n. We claimed that if we consider multiplication modulo n on $U(n)$, then this is a group. We saw that the operation is associative, and that 1 is an identity, and that the Homework problem above guarantees that there are inverse elements. The one question that remains (which was left as an exercise for you) is whether multiplication modulo n takes two elements in $U(n)$, and gives another element in $U(n)$. We now explain why this is true (but be sure you think about this on your own before reading on).

What we would like to show is that if $\gcd(a, n) = 1$ and $\gcd(b, n) = 1$, and

$$ab \equiv c(\text{mod } n),$$

then we also have $\gcd(c, n) = 1$. That is, if a and b have representatives modulo n in the set $U(n)$, then so does their product ab. In particular, this would mean if $a, b \in U(n)$, then $ab\text{mod } n$ is also in $U(n)$, which gives the desired closure property.

We will prove this by contradiction. Assume that $\gcd(c, n) > 1$, which means that $\gcd(c, n)$ must have some prime factor, say p. Then p divides c and n, so we may write $c = px$ and $n = py$ for some $x, y \in \mathbb{Z}$. Now, since $ab \equiv c(\text{mod } n)$, we have n divides $ab - c$. This implies there is an integer m such that

$$ab - c = nm.$$

Since we have $c = px$ and $n = py$, we may rewrite this as $ab = px + pmy = p(x + my)$. Now, we have p divides ab. Since p is prime, then by Euclid's Lemma, $p|a$ or $p|b$. However, $p|n$, and $\gcd(a, n) = \gcd(b, n) = 1$, and so we cannot have $p|a$ or $p|b$, otherwise we would have a contradiction to our original given information. Therefore, we must have $d = 1$.