WORKSHEET # 1 SOLUTIONS

MATH 435 SPRING 2011

1. Consider the set of positive integers $< n$ which are relatively prime to n. We will denote this set by $U(n)$. Show that this set forms an Abelian group under multiplication modulo n.
For example, if $n = 5$, then $U(n) = \{1, 2, 3, 4\}$ and $3 \cdot 4 = 2 \mod n$.

Solution: First let's verify that multiplication mod n really is a binary operation. Suppose that $a, b \in U(n)$. We should check that $ab \mod n$ is relatively prime to n. Now, $(ab \mod n) = ab + qn$ for some $q \in \mathbb{Z}$, so if some prime $d > 1$ divides both n and $(ab \mod n)$, then $d|(ab)$ and since d is prime, it divides a or b. This contradicts the relative primality of n with a and b.

To verify that $U(n)$ is indeed a group, we have three things to check.

(i) Associativity: Choose $a, b, c \in U(n)$. We want to show that $(ab \mod n)c \mod n = a(bc \mod n) \mod n$. Write $(ab \mod n) = ab + mn$ for some $m \in \mathbb{Z}$. Then $(ab+mn)c \mod n = (ab + mn)c + ln = abc + (mc + l)n$. Likewise, $a(bc \mod n) \mod n = a(bc + pn) + qn = abc + (ap + q)n$ for some $p, q \in \mathbb{Z}$. But then clearly $abc + (mc + 1)n \equiv_{\mod n} abc + (qp + q)n$ which proves the result.

(ii) Identity: Obviously $e = 1$ works since $1a = a1 = a$ for any $a \in U(n)$.

(iii) Inverses: Fix $a \in U(n)$. Because $\gcd(a, n) = 1$, there exist integers $s, t \in \mathbb{Z}$ such that $sa + tn = 1$. Working modulo n, we see that $sa \equiv_{\mod n} 1$. But we have thus found our inverse to a, namely $s \mod n$. Of course, we should verify that $\gcd(s, n) = 1$ to see that this inverse is actually in the group. But the equality $as + tn = 1$ in fact implies that $\gcd(a, n) = 1$ as well.

Of course, multiplication of integers (even modulo n) is commutative so the group is indeed Abelian.

Remark: In this problem I constantly identified the element $a \in U(n)$ with its equivalence class modulo n. This is harmless because each equivalence class of integers modulo n has a unique representative in $\{0, 1, \ldots, n-1\}$. We'll be developing some machinery to handle this sort of identification slightly more rigorously in the coming weeks.

2.Additionally, write down complete multiplication tables for $U(5)$ and $U(8)$.

Solution:

U(5)	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

U(8)	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

3. Show that $U(5), U(8)$ and $U(12)$ all have 4 elements. However, also show that $U(5)$ has an element of order 4 but $U(12)$ and $U(8)$ do not.

Solution: We've already found all four elements in $U(5) = \{1, 2, 3, 4\}$ and $U(8) = \{1, 3, 5, 7\}$. Also $U(12) = \{1, 5, 7, 11\}$.

The element 2 has order 4 in $U(5)$ since $2 \cdot 2 \mod 5 = 4 \neq 1$, $2 \cdot 2 \cdot 2 \mod 5 = 3 \neq 1$ but $2 \cdot 2 \cdot 2 \cdot 2 \mod 5 = 1$. Similar computations show that 3 also has order 4 in $U(5)$.

For $U(8)$, we notice that $1^1 = 1$, $3^1 \mod 8 = 1$, $5^2 \mod 8 = 1$ and $7^2 \mod 8 = 1$, thus there are no elements of order 4.

For $U(12)$, we notice that $1^1 = 1$, $5^2 \mod 12 = 1$, $7^2 \mod 12 = 1$ and $11^2 \mod 12 = 1$, thus there are no elements of order 4.

4. Suppose now that G is a group with 4 elements. Show that there cannot be 3 elements of order 4 in G.

Solution: Every group with 4 elements has one element of order 1, the identity. The other 3 elements all have order greater than 1 (since they are not the identity). Suppose that one of those elements, $g \in G$ has order 4 (ie $g^4 = e$ but $g^2 \neq e$ and $g^3 \neq e$). The element $g^2 \in G$ has order 2 since $(g^2)^2 = g^4 = e$. Thus there is an element in the group which does not have order 4. Therefore, all three of the non-identity elements cannot be order 4.