Applied Number Theory: Homework 1

Joshua Dong

September 16, 2016

3

a)

The subgroups of $(\mathbb{Z}/5, +)$ are $(\mathbb{Z}/n, +)$ for all $n \in \{1, 2, 3, 4, 5\}$. The subgroups of $(\mathbb{Z}/10, +)$ are $(\mathbb{Z}/n, +)$ for all $n \in \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$.

Assume m is an integer. Then any element of $m\mathbb{Z}$ is an integer, since integer multiplication is closed. Then $m\mathbb{Z} \subset \mathbb{Z}$.
Let $a_1, a_2 \in m\mathbb{Z}$. Then there exist k_1, k_2 such that $a_1 = mk_1, a_2 = mk_2$. Then $a_1 + a_2 = mk_1 + mk_2 = m(k_1 + k_2)$, by the distributive property of $\mathbb{Z}$ on $(\cdot), +$. Since $\mathbb{Z}$ is closed under addition, $(k_1 + k_2) \in \mathbb{Z}$ and there exists $k \in \mathbb{Z}$ such that $a_1 + a_2 = mk \in m\mathbb{Z}$. Then $m\mathbb{Z}$ is closed under addition.
Since every element of $m\mathbb{Z}$ is an integer, we know that associativity holds in $m\mathbb{Z}$.
Let $a \in m\mathbb{Z}$. Then there exists k such that $a = mk$. Let $b = m(-k)$. $-k \in \mathbb{Z}$ since $\mathbb{Z}$ is a group. Thus $m(-k) \in m\mathbb{Z}$. Then $a+b = mk+m(-k) = mk+-(mk)$, since $(\mathbb{Z}, \cdot)$ is an abelian group. $mk+-(mk) = 0$. Then $a+b = 0$, b is an inverse of a. Then for any $a \in m\mathbb{Z}$, there is an inverse also in $m\mathbb{Z}$.
Since we found an inverse for any element of $m\mathbb{Z}$, a subset of the integers, we know that the identity element is unique since we also showed the set is closed under the group operation.
Then $m\mathbb{Z}$ is a subgroup of $\mathbb{Z}$.

b)

i) The additive cosets of the subgroups $m\mathbb{Z}$ are the numbers of the form $g + mk$ where $g \in \mathbb{Z}$ and k is an arbitrary integer. Since $\mathbb{Z}$ is abelian, the left and right are the same (they are all normal).

ii) The coset gH is a subgroup of G only when g is the identity or the order of H divides g.

iii) Take the set of all cosets of H, denoted V. 0, the identity, is in H. Then for all $g \in G$, there exists an element $v \in V$ containing g, since $g + 0 = g$.

iv) We can create a mapping of any coset of H to any other coset of H. If g_1H, g_2H are a cosets of H, then we create the map $f : g_1H \to g_2H$ where $f(x) = x + (-g_1) + g_2$. This bijection (since we can trivially create f^{-1} which is also injective and surjective) shows that any coset is the same size as any other coset.

v) Suppose $g_1 = g_2$. Then trivially, $g_1H = g_2H$. Suppose $g_1 \neq g_2$.
Suppose x is in g_1H. Then under the equivalence classes of all the left cosets of H, x is in only one of them. Why? If x were in two of them, then for the g_a, g_b left cosets x is in, there would be elements $h_1, h_2 \in H$ such that $g_b + h_2 = x = g_a + h_1$. This implies that $g_b = g_a + (h_1 + (-h_2))$, by the inverse and associative properties of groups. Then clearly, g_b is congruent to g_a under the H coset equivalence class.

c)

Let the order of a subgroup H be denoted $o(H)$, equal to the number of elements in gH, a left coset. Then $o(G)$ is the sum of $o(H)$, disjoint sets, $o(G) = sumforalluniquecosets(o(H))$. Then clearly the order of a subgroup of H divides the order of H.

d)

Fermat's little theorem concerns a mult. group, so the euler's toitient function, or $p-1$ when p is prime, as in this case, forms a multiplicitive ring with $p-2$ elements. As for any a s.t. $a^{p-1} = a^{p-2} \cdot a$, $p-2$ is the order, so a to that power is 1. then 1 times a is clearly a, under the group. formally, a to the power p-2 is equal to a to the power of some xy, integers such that x is the order of a group, thus a to the power x is 1

1.36

2.10