# Math 534 Homework 1

Morgan Gribbins

January 23, 2020

## 1 Prove that $(a +_n b) +_n c = a +_n (b +_n c)$ for $a, b, c \in \{0, 1, ..., n-1\}$, thus finishing our proof from lecture that in the "numbers" definition of $\mathbb{Z}/n$, addition is associative.

Note that $[a] +_n [b] = [a+b]$. Therefore, $([a] +_n [b]) +_n [c] = ([a+b]) +_n [c] = [a+b] +_n [c] = [a+b+c]$. Additionally, $[a] +_n ([b] +_n [c]) = [a] +_n ([b+c] = [a] +_n [b+c] = [a+b+c]$, so both sides are identical.

## 2 Show the following:

### 2.1 For $a, a', b, b' \in \mathbb{Z}$, if $a \cong a' \ (mod\ n)$ and $b \cong b' \ (mod\ n)$, then $ab \cong a'b' \ (mod\ n)$.

By the division algorithm, we can set $a = nq_1 + r_a$, $a' = nq_2 + r_a$, $b = nq_3 + r_b$, and $b' = nq_4 + r_b$. Therefore,

$$ab = (nq_1 + r_a)(nq_3 + r_b) = n^2 q_1 q_3 + nr_a q_3 + nr_b q_1 + r_a r_b$$

$$a'b' = (nq_2 + r_a)(nq_4 + r_b) = n^2 q_2 q_4 + nr_a q_4 + nr_b q_2 + r_a r_b,$$

which are congruent mod n as $r_a r_b \cong r_a r_b \ (mod\ n)$ trivially.

### 2.2 For $a, b, c \in \{1, ..., n-1\}$, show $a \cdot_n (b \cdot_n c) = (a \cdot_n b) \cdot_n c$.

By defining the binary operation $\cdot_n([a], [b]) = [a \cdot b]$, we get $[a] \cdot_n ([b] \cdot_n [c]) = [a] \cdot_n ([b \cdot c]) = [a] \cdot_n [b \cdot c] = [a \cdot b \cdot c]$ and $([a] \cdot_n [b]) \cdot_n [c] = ([a \cdot b]) \cdot_n c = [a \cdot b] \cdot_n c = [a \cdot b \cdot c]$, so the $\cdot_n$ operation is associative.

### 2.3 For $a, c \in \mathbb{Z}$, if $gcd(a, n) = 1$ and $gcd(c, n) = 1$, then $gcd(ac, n) = 1$.

If $gcd(a, n) = 1$, then a and n are relatively prime, and if $gcd(c, n) = 1$, then c and n are relatively prime. The assertion $gcd(ac, n) = 1$ states that ac and n are relatively prime, which directly follows from the prior statements, by the fundamental theorem of arithmetic.

### 2.4 For $a, c \in \mathbb{Z}$, if $gcd(a, n) = 1$ and $a \cong c\ (mod\ n)$, then $gcd(c, n) = 1$.

The proposition that $a \cong c\ (modn)$ implies that a and c vary by an integer multiple of n, i.e. $a = kn + c$ for some integer k. Now, we have $1 = xa + yn$ for integers x,y by hypothesis. Substituting $a = kn + c$ gives us $1 = x(kn + c) + yn = xc + (kx + y)n = 1$, so $gcd(c, n) = 1$ because 1 is the smallest positive integer which can be written as a linear combination of c and n.

## 3 Let $(G, \cdot)$ be a group. For $g \in G$ and $k \in \mathbb{N}$, define $g^k$ as the result of combining g with itself k times using the binary operation of the group. Prove that $(g \cdot h)^2 = g^2 \cdot h^2$ if and only if $g \cdot h = h \cdot g$.

Note that $(g \cdot h)^2 = (g \cdot h) \cdot (g \cdot h) = g \cdot h \cdot g \cdot h$, by the associativity of a group.

Direct proof of ( $\implies$ ):

Assume $(g \cdot h)^2 = g^2 \cdot h^2$. This implies that $g \cdot h \cdot g \cdot h = g \cdot g \cdot h \cdot h$. By applying $g^{-1}$ on the left hand side of the equation and applying $h^{-1}$ on the right hand side of the equation (by cancellation laws), we get

$$g^{-1} \cdot g \cdot h \cdot g \cdot h \cdot h^{-1} = g^{-1} \cdot g \cdot g \cdot h \cdot h \cdot h^{-1} = h \cdot g = g \cdot h.$$

Therefore, $(g \cdot h)^2 = g^2 \cdot h^2 \implies g \cdot h = h \cdot g$.

Direct proof of ( $\impliedby$ ):

Assume $g \cdot h = h \cdot g$. Multiplying on the left of this equation by $g$ and on the right by $h$ gives $g \cdot g \cdot h \cdot h = g \cdot h \cdot g \cdot h$. The left side of this is equivalent to $g^2 \cdot h^2$, and the right side of this equation is equivalent to $(g \cdot h)^2$, which completes our proof via direct implication.

## 4 Let $(G, \cdot)$ be a group.

### 4.1 Show that if $h \in G$ satisfies $h \cdot g = g$ for some $g \in G$, then $h$ is the identity.

Assume that $h \cdot g = g$. Via cancellation laws, apply $g^{-1}$ to the right of this equation to receive $h \cdot g \cdot g^{-1} = g \cdot g^{-1} = h \cdot e = e$, so $h$ is the identity.

### 4.2 Fix $k \in G$. Show that if $h \cdot k = e$, then $h = k^{-1}$.

Assume that $h \cdot k = e$. Applying $k^{-1}$ on both right sides gives $h \cdot k \cdot k^{-1} = e \cdot k^{-1} = h \cdot e = e \cdot k^{-1} = h = k^{-1}$, which is our conclusion.