Assignment 7

Karan Sikka
ksikka@andrew.cmu.edu
E
March 30, 2012

A Long Expected Party

---

a. $(G, [,,])$ follows the rules Lhach and Nar, so it is an Elen. **Proof of Llach**
$[a, b, c] = a \circ b^{-1} \circ c$
$\implies [[a, b, c], d, e] = a \circ b^{-1} \circ c \circ d^{-1} \circ e.$
$[d, c, b] = d \circ c^{-1} \circ b$
$\implies [a, [d, c, b], e] = a \circ (d \circ c^{-1} \circ b)^{-1} \circ e = a \circ b^{-1} \circ c \circ d^{-1} \circ e.$
$[c, d, e] = c \circ d^{-1} \circ e$
$\implies [a, b, [c, d, e]] = a \circ b^{-1} \circ c \circ d^{-1} \circ e$

From the above, it is clear that $[[a, b, c], d, e] = [a, [d, c, b], e] = [a, b, [c, d, e]]$. Therefore, Llach is satisfied.

Proof of Nar
$[a, a, b] = a \circ a^{-1} \circ b = 1 \circ b = b$

$[b, a, a] = b \circ a^{-1} \circ a = b \circ 1 = b$

Since $[a, a, b] = [b, a, a] = b$, Nar is satisfied.

Since Lhach and Nar are both satisfied, $(G, [,,])$ is an Elen.

b. $(A, *)$ is a group if it is closed, associative, contains the identity u, and has an inverse.

Let a, b, and c be in A.

Closure: (to show $a * b \in A$) This is true by the definition of $*$.

Associativity: (to show $a * (b * c) = (a * b) * c$)
$b * c = [b, u, c]$
$\implies a * (b * c) = [a, u, [b, u, c]]$

$a * b = [a, u, b]$
$\implies (a * b) * c = [[a, u, b], u, c]$

By the rule of Lhach, the above two results may be equated, and $(A, *)$ is associative.

Identity: (to show $a * u = a = u * a$)
$a * u = [a, u, u] = a$ (Nar)

$u * a = [u, u, a] = a$ (Nar)

Therefore, $a * u = a = u * a$ and the identity exists.

Inverse: (to show $a * a^{-1} = u = a^{-1} * a$)

$a^{-1} = [u, a, u]$

Right Inverse:
$a * a^{-1} = a * [u, a, u]$ (substitution)
$= [a, u, [u, a, u]]$ (Def of $*$)
$= [a, [a, u, u], u]$ (Llach)
$= [a, a * u, u]$ (Def of $*$)
$= [a, a, u]$ (Identity)
$= u$ (Nar)

Left Inverse:
$a^{-1} * a = [u, a, u] * a$ (Def of $*$)
$[[u, a, u], u, a]$ (Def of $*$)
$= [u, [u, u, a], a]$ (Llach)
$= [u, u * a, a]$ (Def of $*$)
$= [u, u, a]$ (Identity)
$= u$ (Nar)

Since $a * a^{-1} = u = a^{-1} * a$, a^{-1} is an inverse such that $a^{-1} = [u, a, u]$.

Therefore, we have shown that $(A, *)$ is a group.

The Council of Elrond

Let there be n members in the Council, where n is a positive integer. Enumerate the members of the Council in ascending order starting from Frodo with 1. Instead of a circle, put them in a line:

```
1  2  ...  n-1  n
```

Elrond chooses a person, skips k people, and chooses the next person, where k starts at 1 and increases by 1 every iteration. Call $E(k)$ the index of the kth person chosen.

$$E(1) = 1$$

$$E(k) = k + E(k-1)$$

Upon inspection, we see that this is also one more than the sum of positive integers up to k mod n.

$$E(k) = 1 + (\sum_{i=1}^{k} i \mod n) = 1 + (\frac{k(k+1)}{2} \mod n)$$

Claim: When n is a power of two, all members of Elrond are chosen eventually. In mathematical terms, When $n = 2^i$ for some integer i, $E(k)$ will assume all values from 1 to n, where k is a positive number. More strongly, it is true that E(k) will cover all these values using k from 1 to $2k$.

Claim: When n is not a power of two, at least one member of the council of Elrond will never be chosen. In math terms, there exists an m between 1 and n such that $E(k) \neq m$ for all positive integer values of k.

All members of the council will be chosen eventually if there a power of two members in the council.

Battle of the Hornburg

a. Let $a, b \in G$ where G is a group under the operation $*$, with the special property described in the problem. We know $\forall u \in G, u^2 = u * u = e$ where e is the identity, since each element has an order of at most 2. Consider: .

$$
\begin{aligned}
a * b &= e * a * b * e && \text{(identity)} \\
&= b^2 * a * b * a^2 && \text{(order at most 2)} \\
&= b * (b * a)^2 * a && \text{(closure and associativity)} \\
&= b * e * a && \text{(order at most 2)} \\
&= b * a && \text{(identity)}
\end{aligned}
$$

b. To prove that h is a Thalion Gul iff G is abelian, it is sufficient to prove both:

1. If h is a Thalion Gul, then G is abelian.
2. If G is abelian, then h is a Thalion Gul.

Let $a, b \in G$, where G is a group under $*$.

Proof of 1
Let h be a Thalion Gul where $h(x) = x^{-1}$.

From the definition of Thalion Gul, we know $\forall a, b \in G$, $h(a * b) = h(a) * h(b)$. Thus, it follows that:

$$
\begin{aligned}
& h(a * b) = h(a) * h(b) && \text{def of Thalion Gul} \\
\implies & (a * b)^{-1} = a^{-1} * b^{-1} && \text{(def of } h\text{)} \\
\implies & (a * b)^{-1} = (b * a)^{-1} && \text{(definition of inverse)} \\
\implies & h[(a * b)^{-1}] = h[(b * a)^{-1}] && \text{(apply } h \text{ to both sides)} \\
\implies & [(a * b)^{-1}]^{-1} = [(b * a)^{-1}]^{-1} && \text{(inverse of inverse of } u \text{ is } u\text{)} \\
\implies & a * b = b(a && \text{(def of } h\text{)}
\end{aligned}
$$

Thus, we see that if h is a Thalion Gul, then G satisfies commutativity and G is Abelian.

Proof of 2
Let G be Abelian.

Therefore $a * b = b * a$.

$$
\begin{aligned}
h(a * b) &= h(b * a) && \text{(}G\text{ is abelian)} \\
= (a * b)^{-1} &= (b * a)^{-1} && \text{(def of } h\text{)} \\
= b^{-1} * a^{-1} &= a^{-1} * b^{-1} && \text{(Theorem 4)} \\
= h(b) * h(a) &= h(a) * h(b) && \text{def of } h
\end{aligned}
$$

Since $h(a * b) = h(a) * h(b)$, h is a Thalion Gul.

Shelob's Lair

Sym 5 is the group of transformations on the permutations of [5]. We will define the group under the operation of composition ($*$).

Starting from an arbitrary permutation $p \in$ Sym 5, you can transform p to be one of 5! possible permutations. Therefore the order of Sym 5 is $5! = 120$.

G is the group of transformations on the labelings of the graph of Shelob's Lair. We will define the group under the operation of composition ($*'$).

We label Shelob's graph under the following rules. Each node will have an unordered pair of distinct numbers from the set of [5]. Additionally, for all nodes n, n must not have any numbers in common with the neighbors of n. For example, if n is labeled as $\{1, 2\}$, then it's neighbor's labelings must not have 1 or 2.

We will show that G also has order 120. Say you have an arbitrary labeling l. For an arbitrary node n in the graph, choose 2 elements from [5] numbers to represent the node. There are $\binom{5}{2} = 10$ ways to do this. Since n has degree 3, there are 3 other nodes which must have labels, with numbers excluding the first two chosen. So there are $\binom{3}{2} = 3$ different labelings to choose from, and n has 3 neighbors. Therefore, there are 3! ways to label the neighbors of n. For each of these nodes in the neighborset of n, there are 2 neighbors which are not n and only 2 labelings left. Then there are 2 ways to do this step. It is clear to see that there is only 1 way to label the rest of the nodes. In total, that makes

$$10 * 3! * 2 = 120$$

Woah!

$$|G| = |Sym5| = 120$$

Now we will try to show that there exists a function $f : Sym5 \to G$ which is an isomorphism. That is to say there exists a **homomorphism** f which is bijective. To be a homomorphism f must satisfy the property that $f(a * b) = f(a) *' f(b)$ where a and b are elements of Sym 5. Specifically, f is a function which maps a permutation to a labeling of schelob's graph.

Say you have two permutations in Sym 5 called a and b. Recall that $*$ is the composition operator for permutations and $*'$ is the composition operator for graph labelings. If you do $a * b$, you get a permutation c because groups satisfy closure. If you do $f(a)$, you get a graph labeling a'. If you do $f(b)$ you get a graph labeling b'. When you compose these two labelings, you get a labeling c'. Without a thorough proof, $f(c) = c'$.

Bijectivity:
Injectivity:
Say you have two different permutations. Each generates a different graph labeling. Therefore two distinct permutations generate two distinct graph labelings.

This fact, combined with the fact that $|Sym5| = |G|$ leads to the conclusion that the homomorphism is a bijection. Therefore, there exists an isomorphism between Sym 5 and G.

The Siege of Gondor

Part a.
For a given $n \in \mathbb{N}$, consider the consecutive set S of n integers

$$S = \{(n+1)! + 2, (n+1)! + 3, \cdots, (n+1)! + (n+1)\}$$

By the definition of factorial,$\forall k \in \mathbb{N}, 1 \leq k \leq n+1$

$$k|(n+1)!$$

By the definition of divides, for each k, $\exists c \geq 1$ such that:

$$(n+1)! = ck$$

Therefore,

$$(n+1)! + k = ck + k = k(c+1)$$

Therefore, $k|((n+1)!+k)$ by the definition of divides. Therefore, every element in S defined above is composite.

Therefore, S is a set of n composite, consecutive integers which can be generated for any given n. Therefore S exists.

Part b.
First, we prove the following: $x^b - 1 = (x-1)(x^{b-1} + x^{b-2} + \cdots + 1)$

The proof is by algebra:

$$\begin{aligned}(x-1)(x^{b-1} + x^{b-2} + \cdots + 1) &= x(x^{b-1} + x^{b-2} + \cdots + 1) - (x^{b-1} + x^{b-2} + \cdots + 1) \\ &= (x^b + x^{b-1} + \cdots + x) - (x^{b-1} + x^{b-2} + \cdots + 1) \\ &= x^b - 1\end{aligned}$$

Since n is composite, we know $\exists a, b > 1$ such that $n = ab$.

$$2^n - 1 = 2^{ab} - 1 = (2^a)^b - 1$$

Let $x = 2^a$, and then by the result proven above,

$$(2^a)^b - 1 = (2^a - 1)((2^a)^{b-1} + (2^a)^{b-2} + \cdots + 1)$$

The factor on the left is greater than 1, since $a > 1$ and $2^a - 1 \geq 4 - 1 = 3 > 1$. The factor on the right is a sum of positive numbers, each greater than one.

Therefore, if n is composite, $2^n - 1$ can be factored into two integers greater than 1. By definition, it is composite.

Part c.

Mount Doom

Part a.
The proof is by induction.

Claim:
$P(n) =$ "$C_n \geq 2^n$" $\forall n \in \mathbb{N}$

Base Case:
$P(0) \iff C_0 \geq 2^0 \iff 1 \geq 1$
$P(1) \iff C_1 \geq 2^1 \iff \binom{2*1}{1} \geq 2 \iff 2 \geq 2$
The claim holds for the $n = 0$ and $n = 1$.

Inductive Hypothesis:
Assume $P(1) \wedge P(2) \wedge \cdots \wedge P(k)$ for some $k \in \mathbb{N}, \mathbf{k \geq 1}$.

Inductive Step:
(To show $C_{k+1} \geq 2^{k+1}$)

$$
\begin{aligned}
& C_{k+1} \geq 2^{k+1} \\
\iff & C_{k+1} \geq 2^k \cdot 2 && \text{(Algebra)} \\
\iff & C_{k+1} \geq 2C_k && \text{(By the IH)} \\
\iff & \frac{(2k+2)!}{(k+1)!(k+1)!} \geq \frac{2(2k)!}{k!k!} && \text{[Def of } C_n\text{]} \\
\iff & \frac{(2k+2)!}{(k+1)!(k+1)!} \geq \frac{2(2k)!}{k!k!} \cdot \frac{(k+1)(k+1)}{(k+1)(k+1)} && \text{(Multiply by 1)} \\
\iff & \frac{(2k+2)!}{(k+1)!(k+1)!} \geq \frac{2(k+1)^2(2k)!}{(k+1)!(k+1)!} && \text{(Algebra)} \\
\iff & (2k+2)! \geq 2(k+1)^2(2k)! && \text{(Algebra)} \\
& (2k+2)(2k+1) \geq 2(k+1)^2 && \text{(Divide by } (2k)!\text{)} \\
\iff & 4k^2 + 6k + 2 \geq 2k^2 + 4k + 2 && \text{(Expand)} \\
\iff & 2k^2 + 2k \geq 0 && \text{(Simplify)} \\
\iff & \mathit{true} && \text{(k is positive)}
\end{aligned}
$$

Note that since $k \geq 1$, all division above is legal. Since all the steps are reversible, we have proved that $P(k) \implies P(k+1)$.

By mathematical induction, the claim holds.