COL202: Discrete Math **Tutorial 4**

Instructor: Venkata Koppula Release date: 30th August, 2024

The solutions for the ($\star$) marked problems must be submitted on Gradescope by 4th September, 11:59am. The remaining questions can be discussed in class on 2nd September, or on 4th September (12-1pm).

Notations. For any natural number $n \geq 2$, let $\mathbb{Z}_n$ denote the set of natural numbers $\{0, 1, \dots, n-1\}$. We define operations $+_n$ and $\times_n$ on $\mathbb{Z}_n$ as follows:

- for any $a, b \in \mathbb{Z}_n$, $a +_n b = (a + b) \bmod n$.
- for any $a, b \in \mathbb{Z}_n$, $a \times_n b = (a \cdot b) \bmod n$.

The set $\mathbb{Z}_n^* = \{k \in \mathbb{Z}_n \setminus \{0\} \ : \ \gcd(k, n) = 1\}$, and the size of $\mathbb{Z}_n^*$ is denoted by $\phi(n)$.

For the rest of this tutorial, p denotes a prime number.

1 Tutorial Submission Problem ($\star$)

In this problem, we abstract out the properties that were used for proving Fermat's Little Theorem and Lagrange's Theorem. Recall, in both these proofs, we did not use the $+_p$ operation (we only used the properties related to $\times_p$). Here, we formally define a set with just one associated operation.

Definition 1. *A finite multiplicative group is a finite set G with an associated operation $\otimes$ (analogous to $\times_p$) with the following properties:*

1. *There exists an element $e \in G$ (analogous to $1 \in \mathbb{Z}_p$) such that for all $a \in G$, $e \otimes a = a \otimes e = a$.*
2. *For all $a, b \in G$, $a \otimes b \in G$.*
3. *For all $a, b, c \in G$, $a \otimes (b \otimes c) = (a \otimes b) \otimes c$.*
4. *For all $a \in G$, there exists $b \in G$ such that $a \otimes b = e$.*

Note that this set G can be any set, and therefore we cannot use PMI. Also, in class, we used the commutativity property, but this property may not be available for all multiplicative groups. We will prove the following theorems for $(G, \otimes)$.

1. Take any element $a \in G$. Consider the following set H_a:

$$H_a = \{e, a, a \otimes a, a \otimes a \otimes a, \dots\}$$

This is a finite subset of G. Prove that this finite subset is also a multiplicative group (that is, it satisfies the four properties listed above). The first three properties are immediate from the definition of H_a. Prove the existence of an inverse for every element in H_a.

2. Suppose $H_a \neq G$ (that is, H_a is a proper subset of G). Take any $b \in G \setminus H_a$, and consider the set $I_{a,b}$ defined as follows:

$$I_{a,b} = \{b \otimes z \ : \ z \in H_a\}$$

What can you say about $H_a \cap I_{a,b}$? Similarly, take any two elements $b, b' \in G \setminus H_a$. What can you say about $I_{a,b} \cap I_{a,b'}$?

3. Let $\mathsf{ord}(a) = |H_a|$. Use Part (2) to conclude that $\mathsf{ord}(a)$ divides $|G|$. You have proven Lagrange's Theorem for general multiplicative groups.

4. Let $\exp_G(a, d) = a \otimes a \otimes \ldots \otimes a$, where the multiplication is performed d times. Use Part (3) for proving that $\exp_G(a, |G|) = e$. You have proven Fermat's Little Theorem for general multiplicative groups.

2 Problems

2.1. I have four pet dogs, five pet cats and four pet rabbits at home (and all of them can do computations modulo 97). I want to share a secret $s \in \mathbb{Z}_{97}$ such that any of the following combinations can recover the secret, but no other combination should learn anything about the secret:

- two dogs and three cats
- one dog, two cats, two rabbits
- three dogs and two rabbits

Suggest a secret sharing scheme for achieving the above. Note that the only allowed operations for reconstructing the secret are $+_{97}$ and $\times_{97}$.

2.2. In this problem, we will compute $\phi(k)$ for any $k \in \mathbb{N}$, $k \geq 2$. First, note that if p is prime, then $\phi(p) = p - 1$.

1. Let m, n be natural numbers such that $\gcd(m, n) = 1$. Prove that $\phi(m \cdot n) = \phi(m) \cdot \phi(n)$.
2. Let $k \in \mathbb{N}$ and p be a prime. Show that $\phi(p^k) = p^{k-1} \cdot (p - 1)$.
3. Give an expression for $\phi(n)$ (use the prime factorization of n).

2.3. Let $n = p \cdot q$ where p and q are primes, and let d, e be natural numbers such that $d \cdot e \bmod (\phi(n)) = 1$. Prove that, for all $x \in \mathbb{Z}_n$, $\exp_n(\exp_n(x, e), d) = x$.

(Hint: if $x \in \mathbb{Z}_n^*$, then this should follow from Euler's theorem discussed in Lecture 11. What if $x \in \mathbb{Z}_n \setminus \mathbb{Z}_n^*$?)

2.4. Consider the following predicate:

n = 6 div by 59

$P(n)$:= let $p_1, p_2, \ldots, p_n$ be the first n prime numbers. Then $p_1 \cdot p_2 \cdot \ldots \cdot p_n + 1$ is prime.

Is this predicate true? Either prove, or find a counterexample.

✓ 2.5. Prove that there exist exactly two elements in $\mathbb{Z}_p$ that satisfy the following equation:

$$\exp_p(x, 2) = 1.$$

Use this (or otherwise) to conclude the following identity:

$$1 \times_p 2 \times_p \ldots \times_p (p-1) = p-1$$

✓ 2.6. Let n be a composite number. What are the possible values for the following:

$$1 \times_n 2 \times_n \ldots \times_n (n-1)$$

Hint: try a few examples, then propose a claim and prove it.

✓ 2.7. Let $n = p \cdot q$, where p and q are primes greater than 30. Give an upper bound on the number of solutions in $\mathbb{Z}_n$ that the following equation can have, and discuss how to find these solutions efficiently (in time $\mathsf{polylog}(n)$).

$$(x-1) \times_n (x-2) \times_n (x-3) = 0$$

✓ 2.8. Prove that for all $n \in \mathbb{N}$, 42 divides $n^7 - n$.

✓ 2.9. Let p be an odd prime. For any $a \in \mathbb{Z}_p$, the Legendre symbol $\left(\frac{a}{p}\right)$ is defined as follows:

$$\left(\frac{a}{p}\right) = \begin{cases} 0 \text{ if } a = 0 \\ 1 \text{ if } \exists x \in \mathbb{Z}_p \text{ such that } x \times_p x = a \\ -1 \text{ otherwise} \end{cases}$$

1. Prove that $\left(\frac{a}{p}\right) = \exp_p(a, (p-1)/2)$.
2. Show that there are exactly $(p-1)/2$ elements in $\mathbb{Z}_p$ such that $\left(\frac{a}{p}\right) = 1$.
3. Show that for all $a, b \in \mathbb{Z}_p$, $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{a \cdot b \bmod p}{p}\right)$

This is version 1.0 of the tutorial sheet. Let me know if something is unclear. In case of any doubt or for help regarding writing proofs, feel free to contact me or TAs.

Venkata Koppula - kvenkata@iitd.ac.in
Ananya Mathur - cs5200416@iitd.ac.in
Anish Banerjee - cs1210134@cse.iitd.ac.in
Eshan Jain - cs5200424@cse.iitd.ac.in
Mihir Kaskhedikar - cs1210551@iitd.ac.in
Naman Nirwan - Naman.Nirwan.cs521@cse.iitd.ac.in
Pravar Kataria - Pravar.Kataria.cs121@cse.iitd.ac.in
Shashwat Agrawal - csz248012@cse.iitd.ac.in
Subhankar Jana - csz248009@iitd.ac.in