Math 319NT Fall 2024 **Name: Aby Soumare**
Lab 5: Wilson's Theorem and Primality Test
Collaborators:

Introduction

In this lab, we were tasked with trying to prove Wilson's Theorem with the resources provided by Professor Tori Day and Magma. Wilson's Theorem is about how $(p-1)!$ behaves when $\mod p$, also the opposite holds true. Meaning, we are able to take a number n and if $(n-1)! \equiv 0 \mod n$ or $(n-1)! \equiv -1 \mod n$ is true, then we know n is prime. One test that we will dive into later in the paper is how to use our findings of Wilson's theorem to determine if a given number is prime.

Background

Before going into discoveries and observations, however, there are some ideas and terms that need to be known. First, we must know what it means for $a \equiv b \mod n$. Consider this definiton:

Definition 0.1. *For an integer a to be equivalent, $\equiv$, to another integer, b, with a modulus n, we write:*

$$a \equiv b \mod n.$$

What this means is that in the division algorithm, these two numbers have the same remainder. So, to generalize, we would write:

$$a = nm + r,\ b = qm + r.$$

For some numbers $n, q \in \mathbb{Z}$.

Exercise 0.1. $11 \equiv 6 \mod 5$,
$11 \mod 5 = 1$,
$6 \mod 5 = 1$.

Keep this fact in mind for the rest of this report. Another term we should familiarize ourselves with is **Z**$/n$. Look at this example:

Exercise 0.2. ***Z***$/5$*:*
$\{0, 1, 2, 3, 4\}$,
and if I were to input 6 into ***Z***$/5$*, then 6 would then become 1.*

As you can see, it is very similar to modding a number, but we are just making a group out of the possible solutions to a number $\mod n$. To put this into a general form, the group **Z**$/n$ would have elements:

$$\{0, 1, 2, 3, ..., n-1\}.$$

For addition and multiplication on the group $\mathbb{Z}/n$, we would do the same process as we would in the regular integers, but the remainder would then be the value we attribute to that operation. Recall the division algorithm, the remainder in the division algorithm would be the value for the operation. For addition, you can see this example:

Example 0.2. *Consider* $\mathbb{Z}/7$*,*
$10 + 14 \mod 7 \equiv 24 \mod 7 = 3.$

Analysis

One of the first exercises professor Tori Day had us do was to play around with Magma to better understand the $\mod$ function. Look at the work done here:

Exercise 0.3. *Exercise 1 and 2:*

- $x := 2 \mod 5;$
- $y := 3 \mod 5;$
- $x + y;$ *returned 5.*

The reason Magma returned 5 in this case was because we didn't tell magma to be thinking in **Z**$/5$. Sure, both x and y were numbers $\mod 5$, but $2, 3 \mod 5$ are the same in **Z**$/5$ and **Z**. If we told Magma to be thinking of these numbers in **Z**$/5$ then the result would be 0.

Now, let us play with $(p-1)! \mod p$ to try and understand it more:

Exercise 0.4. *Exercise 3:*
Choose your favorite prime, p *and use Magma to compute* $(p-1)! \mod p$*:*
$p = 11, (11-1)! \mod 11 = 10,$
$p = 7, (7-1)! \mod 7 = 6.$

As one may notice, the result of $(p-1)! \mod p$ is $p-1$, so:

Exercise 0.5. *Exercise 4: Write a conjecture of the form* $(p-1) \equiv x \mod p$*:*
$(p-1)! \equiv p-1 \mod p,$
$(p-1)! \equiv -1 \mod p.$

This is Wilson's Theorem. So:

Theorem 0.3. *Let* p *be a prime number.* $(p-1)! \equiv -1 \mod p.$

In these next exercises, we will be further proving this theorem. Consider:

Exercise 0.6. *Let* p *be a prime. Let* $a \in \mathbb{Z}/p$ *such that* $a^2 \equiv 1 \bmod p$*. Then* $a = \pm 1$*.*

Proof. Since we know $a^2 \equiv 1 \bmod p$, we know $p | a^2 - 1$. So, consider:

$$a^2 - 1 = (a+1)(a-1).$$

Now, we can continue to say that

$$p | (a+1)(a-1).$$

So, we will continue by solving each factor separately by Euclid's Lemma. Consider $(a+1)$:

$$\begin{aligned} a+1 &\equiv 0 \bmod p \\ a &\equiv -1 \bmod p. \end{aligned}$$

Now on to $(a-1)$:

$$\begin{aligned} a-1 &\equiv 0 \bmod p \\ a &\equiv 1 \bmod p. \end{aligned}$$

Therefore, $a = \pm 1$. □

Now, we can continue on to finally proving Wilson's Theorem.

Exercise 0.7. *Prove Wilson's Theorem.*

Proof. We know $(p-1)! = (p-1)(p-2)...(2)(1)$. Via our last example, we know that if we were to group all of those roots together such that

$$a * a^{-1} \equiv 1 \bmod p$$

for all elements $\in \mathbb{Z}/p$, then when we continue throughout the entire set of elements, all will simplify down to 1. However, this pattern changes when we get to the last elements in $\mathbb{Z}/p$, where $1(p-1) \equiv -1 \bmod p$. Since all other elements are 1, then we know that $(p-1)! \equiv -1 \bmod p$, and have therefore proven Wilson's Theorem. □

Now, in order to create a primality test related to Wilson's Theorem, we are going go prove this lemma:

Lemma 0.4. *If $n \geq 6$ is composite, then $(n-1)! \equiv 0 \bmod n$.*

In order to prove this, the process was broken down into multiple steps to ease the pain a little. First, consider this exercise:

Exercise 0.8. *Suppose n is not the square of a prime p, so $n = ab$ with $1 < a < n$ and $1 < b < n$. Show that $(n-1)! \equiv 0 \bmod n$.*

Proof. Since we know that $ab = m$ and also $a, b \in \mathbb{Z}/n$, then consider:

$$(n-1)! = 1 * 2 * ... * a * b * ... * (n-1),$$

written as

$$\begin{aligned} (n-1)! &= a * b(1 * 2 * ... * (n-1)) \\ &= n(1 * 2 * ... * (n-1)). \end{aligned}$$

Since all multiples of n in $\mathbb{Z}/n$ will be $\equiv 0 \bmod n$, then we know that $(n-1)! \equiv 0 \bmod n$. □

Now, let's go on to the next step in proving the Lemma. Consider this exercise:

Exercise 0.9. *Suppose n is the square of a prime so that $n = p^2$. Note that since $n \geq 6$, $p \geq 3$. Show that $(n-1)! \equiv 0 \bmod p$.*

Proof. So, we know that the elements of $\mathbb{Z}/n$ are,

$$(n-1)! = 1 * 2 * 3 * ... * p * ... * (n-1).$$

So we can consider:

$$(n-1)! = p(1 * 2 * 3 * ... * (n-1).$$

Since we know that $n = p^2$, then we know that $2p \in \mathbb{Z}/n$ since $p^2 > 2p$ for $p > 2$ (since $p^2 > 2p$ doesn't hold when $p = 2$). So, we can pull out the other p from the element $2p$ to get:

$$(n-1)! = p * p(1 * 2 * 3 * ... * 2 * ... * (n-1).$$

Note that the extra 2 shown in the last equation is the left-over 2 from the $2p$ we took the p from. Since $p * p \equiv 0 \bmod n$, then we know that $(n-1)! \equiv 0 \bmod n$. □

After proving those two exercises, we can see that this primality test isn't the greatest for us to be using all the time. Namely, this is going to be incredibly slow for our computers to compute for very large numbers. However, we are still going to play around with it a bit here.

Exercise 0.10. *Use your WilsonPrimeTest function to determine if 3 numbers larger than 100 are composite.*

```
   > WilsonPrimeTest(101);
prime
> WilsonPrimeTest(444);
composite
> WilsonPrimeTest(22221);
composite
> WilsonPrimeTest(28337913);
composite
```

Future Directions

After exploring the topic within this lab, a couple questions arise. Namely, is there a more efficient way to find primes using Magma? Why would anyone use this specific test over any other prime test? Also, since new technologies, namely AI, are makign a break in the math world, is being able to understand these kinds of tests going to be useful in the future?

Most of these questions we do not yet have the answer to, however they are interesting to ponder over.

Appendix

Code 0.5. *Conjecture Code:*

```
for p in PrimesUpTo[100] do
    R:= Integers(p);
    x:= Factorial(p-1);
    R!x;
    return x, p;
end for
```

Code 0.6. *Wilson Primality Test:*

```
function WilsonPrimeTest(n)
    R:= IntegerRing(n);
    x:= Factorial(n-1);
    y:= R!x;
    if y eq 0 then
        return "composite";
    else
        return "prime";
    end if;
end function;
```