Prime Numbers

PLEASANTON MATH CIRCLE

November 3rd, 2016

1 Introduction

The aim of this meeting is to provide exposure to a bunch of results regarding prime numbers. Some of these results are easy to prove. Some are hard to prove. Others haven't been proved! We begin with a very important definition.

Definition 1 (Prime Numbers)**.** A **prime number** is a positive integer that has exactly 2 divisors: 1 and itself.

Exercise 2. List the first 10 prime numbers.

We also define what the composite numbers are.

Definition 3 (Composite Numbers)**.** A **composite number** is a positive integer that has more than 2 divisors.

One thing to remember is that 1 is considered to be neither prime nor composite.

Exercise 4. List the first 10 composite numbers.

Now that you know some important definitions, try some of these problems.

Exercise 5 (Triple Prime Conjecture)**.** Find all positive integers n such that $n, n+2$, and $n+4$ are all prime.

Exercise 6. Find an integer x such that $3x^{2016} + x^{2015} + 4x^{2014} + x^{2013} + 5x^{2012} + 9$ is not a prime.

2 Infinitude of Primes

One of the first questions you can ask about primes is *how many are there*? It turns out that there are a lot. Specifically ...

> **Theorem 7** (Infinitude of Primes)
> There are an infinite number of primes.

Exercise 8. Prove Theorem 7. Hint: Assume that there are a finite number of primes $p_1, \ldots, p_n$ and then try to find a contradiction.

3 Fermat's Little Theorem

Fermat's Little Theorem is one of the most fundamental (and famous) theorems in number theory. It involves the divisibility of numbers raised to a prime power.

Exercise 9. What is the remainder when 2^3 is divided by 3? What is the remainder when 2^5 is divided by 5?

Exercise 10. What is the remainder when 4^3 is divided by 3? What is the remainder when 5^3 is divided by 3? What is the remainder when 8^3 is divided by 3? What is the remainder when x^p is divided by p if p is a prime?

Theorem 11 (Fermat's Little Theorem)
Let a be a positive integer that is not divisible by a prime p. Then $a^p - a$ is divisible by p.

Now we will try to prove this. First we will show that it is true in the case where $a = 2$ and $p = 5$. There are 32 5 letter words can you make that have only A's and B's.

$AAAAA$	$AAAAB$	$AAABA$	$AAABB$	$AABAA$	$AABAB$	$AABBA$	$AABBB$
$ABAAA$	$ABAAB$	$ABABA$	$ABABB$	$ABBAA$	$ABBAB$	$ABBBA$	$ABBBB$
$BAAAA$	$BAAAB$	$BAABA$	$BAABB$	$BABAA$	$BABAB$	$BABBA$	$BABBB$
$BBAAA$	$BBAAB$	$BBABA$	$BBABB$	$BBBAA$	$BBBAB$	$BBBBA$	$BBBBB$

We call two words *friends* if one word can be rotated (meaning each letter moves down and the last one becomes the first) to get the other word. For example, $ABAAB$ and $AABAB$ are friends.

Exercise 12. How many words are there? Why?

Exercise 13. Group friends together. Do you notice any patterns?

Exercise 14. Show why Fermat's Little Theorem is true in this case. Can you see why its true in general?

4 More Problems to Think About

Here are some more problems related to the material discussed so far.

1. How can you check if a number is prime? Can you improve your method? Using this method, can you think of a way to generate all prime numbers?

2. Fermat's Little Theorem can also be stated as $a^{p-1} - 1$ is divisible by p when a is not divisible by p. The Mersenne primes are primes of the form $2^n - 1$. For what n is $2^n - 1$ not prime?

3. Can you generate any other interesting prime number properties?