1 Introduction

Our goal today is to learn about various results and questions regarding prime numbers, some of which will be easy to prove, while others will be harder. Yet others have not even been proved yet! But first, a reminder of the definition of a prime number:

Definition 1. A **prime number** is a number that only has two divisors: 1 and itself.

Numbers that are not prime are called composite numbers.

Definition 2. A **composite number** is a number with more than two divisors.

1.1 Exercises

Exercise 1. Is the number 35 a prime or composite number?

Exercise 2. Is the number 37 a prime or composite number?

Exercise 3. Is the number 1 a prime or composite number?

1.2 Easier Check for primes

To determine if N is prime, we only need to check divisors that are less than $\sqrt{N}$.

Exercise 4. Is 397 prime?

2 Number of primes

You might be wondering, how many primes are there? It has been known since the ancient Greeks that there are, in fact, an infinite number of primes:

Theorem 1. There are an infinite number of primes.

2.1 Exercises

Exercise 5. Prove Theorem 1 (Hint: Try using contradiction)

Exercise 6. Consider the sequence of numbers of the form $4k + 3$:

$$3, 7, 11, 15, 19, 23, 27, 31, 35, 39, 43 \dots$$

Do you think there are infinitely many primes in this sequence? Prove it!

3 Fermat's Little Theorem

One of the most fundamental theorems in number theory is **Fermat's Little Theorem**. If you study more number theory (which you totally should), you will definitely encounter it again. It is a statement about a nice relationship involving divisibility and numbers raised to a prime power. In order to motivate it, try the next couple of exercises:

Exercise 7. What is the remainder when 2^3 is divided by 3? What is the remainder when 2^5 is divided by 5? When 2^7 is divided by 7?

Exercise 8. What is the remainder when 4^3 is divided by 3? When 5^3 is divided by 3? When 7^3 is divided by 3?

Exercise 9. Can you generalize your results from the previous two exercises?

The result is the following nice little theorem:

Theorem 2. (Fermat's Little Theorem) If p is a prime number and a is a natural number, then

$$a^p \equiv a \pmod{p}$$

Over the next few exercises, we hope you gain an intuition for why Fermat's Little Theorem is true. Consider the case when $a = 2$ and $p = 5$. We can think of a^p then as the number of 5-letter words we can form from the letters A and B:

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

Let us call two words *friends* if the letters in one word can be shifted to produce the other. For example, $AAABA$ is friends with $AAAAB$, because shifting every letter of $AAABA$ one place to the right, where the last letter "wraps around" to the beginning of the word, gives $AAAAB$.

Exercise 10. First off, how many words are there?

Exercise 11. Group words that are friends together. Do you notice anything interesting? Can you see then why Fermat's Little Theorem is true in the case of $a = 2$ and $p = 5$?

Exercise 12. Can you see why Fermat's Little Theorem is true for any prime p and any number a?

3.1 Exercises

Exercise 13. What is the remainder when 4^{11} is divided by 11?

Exercise 14. What is the remainder when 23^{19} is divided by 19?

Exercise 15. What powers x can 5 be raised to so that 5^x divided by x yields a remainder of 5?

Exercise 16. (AMC 12 2008 12A) Let $k = 2008^2 + 2^{2008}$. What is the units digit of $k^2 + 2^k$?

4 More exercises

Exercise 17. (Prime triplets) Find all positive integers n such that n, $n + 2$, and $n + 4$ are all prime.

Exercise 18. Earlier, we mentioned that to check if a number N is prime, one only needs to check numbers up to $\sqrt{N}$. Explain why this is the case!

Exercise 19. Plug some values into the expression $n^2 - n + 17$. What do you notice about the numbers?

Exercise 20. Do you think this holds for any n? If so, prove it! If not, find a counterexample!

Exercise 21. Replace 17 with another prime number, and repeat the two previous exercises. Do you think there exists a prime p such that $n^2 - n + p$ *always* gives primes? How about an expression that always gives primes?

5 Interesting Facts/Occurrences

1. The number 73,939,133 is prime, but chopping off one digit at a time from the right also leaves prime numbers!
2. The largest prime number found so far has $23,249,425$ digits
3. Circle the primes in Figure 1. Do you notice anything about their locations? The same thing, but on a much larger scale, is shown in Figure 2.

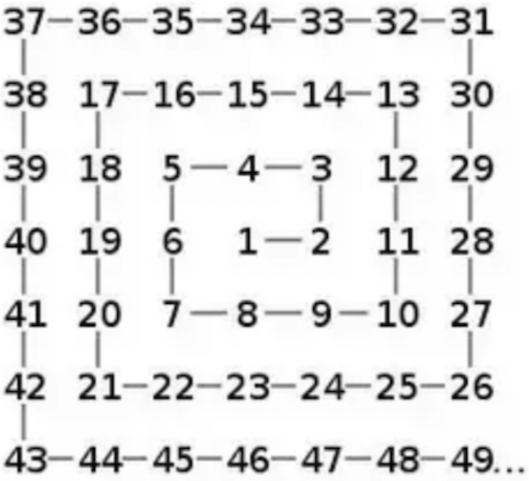

Figure 1: Ulam spiral

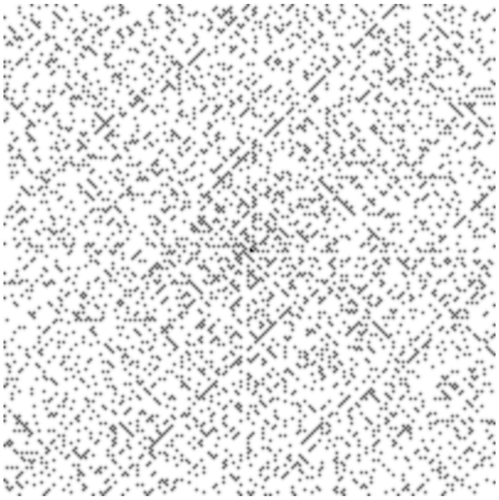

Figure 2: Large Ulam spiral

4. In exercise 6, you showed that in the sequence of numbers of the form $4n+3$, there are infinitely many primes. A natural follow up to this is to generalize and ask whether infinitely many primes also appear in the sequence $an+d$, where a and d are some integers. It turns out that whenever a and d are relatively prime[1], the sequence $an+d$ always hits infinitely many primes.

5.1 Unsolved Problems

Finally, to give you a sense of how something so simple like primes can lead into difficult questions, here are some questions that are still today unknown:

1. (Twin prime conjecture) In exercise 17, you found that there is only one prime triplet. Naturally, you might wonder how many pairs of primes there are that differ by 2, like $(3,5)$, $(5,7)$, or $(11,13)$. Using computers, mathematicians have found twin primes as large as $\approx 10^{390,000}$. Yet, it is in fact still unknown whether there are infinitely many twin primes.
2. (Mersenne Primes) Mersenne Primes are defined as primes that can be written as 2^n-1. It is still not known whether or not the set of Mersenne Primes is infinite or finite.
3. (Goldbach's conjecture) States that every even integer greater than 2 can be written as a sum of two primes. Using computers, the conjecture has been verified for even numbers up to $\approx 4 \cdot 10^{18}$. Yet, we do not know whether this will hold for all even numbers.
4. (Legendre's conjecture) Does there always exist a prime between consecutive perfect squares?

[1] Two numbers are **relatively prime** if the only positive integer that divides both of them is 1.