1 Algebra and Number Theory

Definition: A number p is prime if it is only divisible by one and itself.

Definition: A number is composite if it is not prime.

Fundamental Theorem of Arithmetic: Every integer n can be represented uniquely as a product of powers of primes. (Prime Factorization)

Question: Using the Fundamental Theorem of Arithmetic, prove there are infinitely primes. (Hint: First try assuming there are only finitely many primes.)

Definition: Two numbers m and n are called relatively prime or coprime if they share no commons factors except for 1 i.e. $\gcd(m,n) = 1$.

Question: What is the probability that an integer a is divisible by a prime p?

Question: What is the probability that two integers are divisible by a prime p?

Question: What is the probability that s integers are divisible by a prime p?

Question: What is the probability that at least one of the s integers is not divisible by a prime p?

Definition: Two prime numbers p and q are called twin primes if they differ by 2.
Fermat's Little Theorem: For a prime number p and an integer a,

$$a^p = a \mod p.$$

Question: What happens when a and p are coprime?

Question: When is the reverse of the above theorem true?

Definition: The set of integers modulo n, $\{0, 1, 2, ..., n-1\}$ is denoted $\mathbb{Z}_n$. In most choices for n there exists two distinct nonzero numbers that multiply to zero.
Question: Do examples exist for the following cases?

1. $\mathbb{Z}_8$
2. $\mathbb{Z}_5$
3. $\mathbb{Z}_{10}$
4. $\mathbb{Z}_{17}$
5. $\mathbb{Z}_{24}$
6. $\mathbb{Z}_{50}$
7. $\mathbb{Z}_{11}$

We could do this all day for infinitely many choices of n. The trick is that when n is prime two such numbers do not exist. In fact $\mathbb{Z}_p$ is an example of a field. Other examples include the real numbers $\mathbb{R}$ and complex numbers $\mathbb{C}$.

2 Finding Primes

Being able to find prime numbers has been the focus of intense research for centuries. Especially today when the use of very large prime numbers is used in data encryption. We now see different ways of finding prime numbers and determine any patterns.

Sieve of Eratosthenes: The slowest way to find primes is be first using this technique and appeals to the Fundamental Theorem of Arithmetic. This process involves listing out the integers in order and then starting with 2 and marking out all multiples of 2, next marking out all multiples of 3, and then continuing in this manner with known primes or numbers not marked out by the sieve. This process is very tedious and is very quickly limited by the space to write.
First list the numbers in order,

$$1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, ...$$

Next mark out multiples of 2,

$$1, 2, 3, \cancel{4}, 5, \cancel{6}, 7, \cancel{8}, 9, \cancel{10}, 11, \cancel{12}, 13, \cancel{14}, 15, \cancel{16}, 17, \cancel{18}, 19, \cancel{20}, ...$$

Now the multiples of 3,

$$1, 2, 3, \cancel{4}, 5, \cancel{6}, 7, \cancel{8}, \cancel{9}, \cancel{10}, 11, \cancel{12}, 13, \cancel{14}, \cancel{15}, \cancel{16}, 17, \cancel{18}, 19, \cancel{20}, ...$$

Since 4 has been sieved already we would now continue with multiples of 5 and then continuing down the list.

Formulas for Primes:

1. Euler discovered that the function

$$f(n) = n^2 - n + 41$$

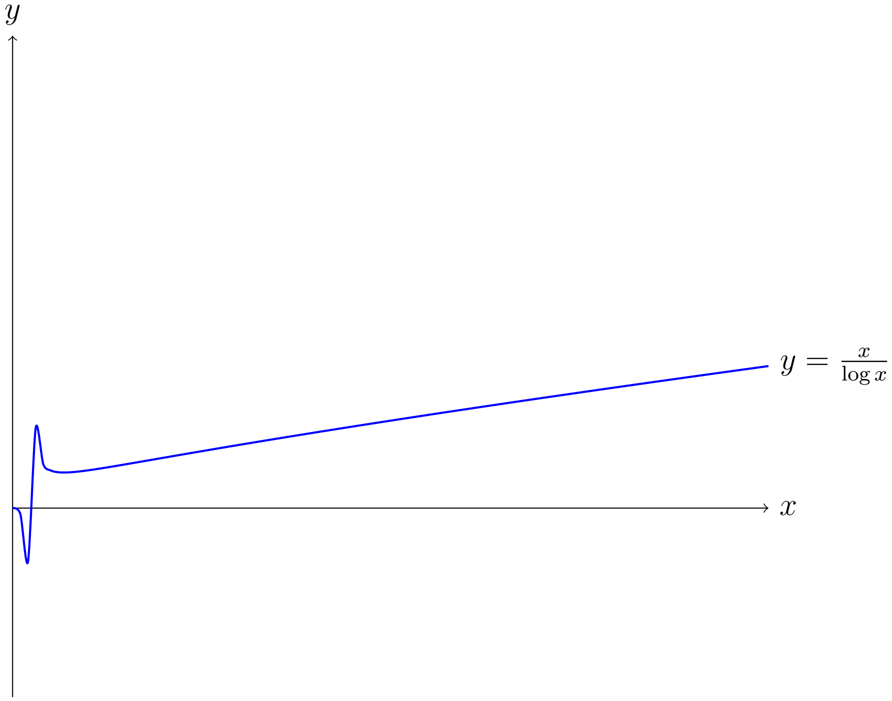
   is prime for every integer less than than 41. Without too much work we can see that $f(41) = 41^2 - 41 + 41 = (41)(41)$ which is clearly not prime.

2. **Mersenne Primes:** These are prime numbers of the form $2^n - 1$ for a prime number n. It is not true that for every prime number p that $2^p - 1$ is also prime. Example when $n = 11$,

$$2^{11} - 1 = 2047 = (23)(89).$$

Question: Why cant $2^n - 1$ be prime when n is composite?

3. **Prime Number Theorem:** If $\pi(n) =$ (number of prime numbers less than or equal to n) then the asymptotic behavior (as n grows towards ∞) is that $\pi(n) \sim \frac{n}{\log n}$



3 Analysis (Calculus)

Definition: The Gamma Function is defined as for $\Re(z) > 0$,

$$\Gamma(z) = \int_0^\infty x^{z-1} e^{-x} dx.$$

An interesting fact about this function is that $\Gamma(z+1) = z\Gamma(z)$. Along with the fact that $\Gamma(1) = 1$ we see that $\Gamma(n) = (n-1)!$. This function is seen as an extension of the factorial operation for non-integers. But how does this function relate to prime numbers? We can define another function in terms of $\Gamma(z)$ that can viewed as an infinite product indexed over Primes!!

Definition: The Riemann Zeta Function is defined as

$$\zeta(z)\Gamma(z) = \int_0^\infty \frac{x^{z-1}}{e^x - 1} dx,$$

and when $\Re(z) > 1$ we get the convergent series

$$\zeta(z) = \sum_{n=1}^{\infty} \frac{1}{n^z}$$

The second definition will be the one we are concerned with.
Question: When the above series makes sense show that

$$\zeta(z) = \prod_{p \text{ prime}} \frac{1}{1 - p^{-z}.}$$

(Hint: First try subtracting $\frac{1}{2^z}\zeta(z)$ from $\zeta(z)$

Question: Write the probability of s integers being coprime in terms of the zeta function.

Related to both the Prime Number Theorem and Riemann Zeta Function is the famously unsolved conjecture which states that,

Riemann Hypothesis: The only non-trivial zeroes of $\zeta(z)$ occur when $\Re(z) = \frac{1}{2}$. But why is this such a big deal, if the above conjecture is true it was shown that the asymptotic behavior of $\pi(x)$ behaves like

$$\int_2^x \frac{dt}{\log t} + \mathcal{O}(\sqrt{x} \log x).$$

Knowing a very good bound on the distribution of primes poses threats to security and encryption such as RSA which relies on the product of two large primes and breaking the code involves figuring out which two primes were chosen.

4 Challenge Questions

Question: What is the value of $\Gamma(\frac{1}{2})$?

Question: What is a formula for $\Gamma(\frac{2n+1}{2})$ for n an integer. (Hint: Use the above question and properties of $\Gamma(z)$.

Question: What is a way to define $\Gamma(z)$ for $\Re(z) < 0$? (Hint: Think recursively)

Question: Ask about Prime Ideals then show that all polynomials with even coefficients is a prime ideal of $\mathbb{Z}[x]$.

Question: Can you think of anymore examples of Prime Ideals?