Rationals are Countable

Let's look at a subset of the reals: $R^* = [0, 1)$

Assume the existence of an bijective function, $f: R^* \rightarrow \mathbb{N}$

Diagonalization Argument

Reals are not Countable

Let's look at a subset of the reals: $R^* = [0, 1)$

Assume the existence of an bijective function, $f: R^* \rightarrow \mathbb{N}$

Diagonalization Argument

Infinite Hierarchy of Infinities

|\mathbb{N}| = \aleph_0

Given an infinite set $S$, the powerset of $S$, $P(S)$, is of higher cardinality

- Diagonalization argument

We say $\aleph_i$ is the next largest set size after $\aleph_{i-1}$

Continuum hypothesis:

- There is no set whose size is between that of the integers and that of the reals
Halting Problem

Assume there exists routine:
- Boolean Halt(String program, String input) (returns true if program executed on input halts, false otherwise)
- We can write:
  ```java
  Boolean trouble(String program) {
    if Halt(program, program)
      return false;
    else
      while (true) ;
  }
  ```

Diagonalization:

Rationals and Irrationals

Rationals are closed under addition, subtraction, multiplication, and division
- Irrationals are not closed under multiplication
  - Irrational * irrational may equal rational
  - What about irrational * (non-zero) rational?

Mersenne Primes

Primes of the form $2^n-1$
- For example: 3, 7, 31, 63
- Any such prime must actually be of the form $2^p-1$
  - Because $2^{km}-1 = (2^m-1)(2^{km-1} + 2^{km-2} + \ldots + 1)$
- 38th known Mersenne prime: $2^{6,972,593}-1$
  - Contains >2,000,000 digits

Sieve of Eratosthenes

Make a list of natural numbers
- Circle the first number, 2, and mark all its multiples

Repeat
- Circle the first uncircled unmarked number
- Mark all its multiples
- Circled numbers are prime
Floor and Ceiling

Ceiling(x): \( \lceil x \rceil \)
- The least-integer greater than or equal to x

Floor(x): \( \lfloor x \rfloor \)
- The greatest-integer less than or equal to x

Graph:

Modulo

Remainder when dividing two positive integers (mod as an operator):
- \( n = m \cdot \lfloor n \div m \rfloor + (n \mod m) \)

Extended to negative numbers (\( y \neq 0 \))
- \( x \mod y = x - y \cdot \lfloor x \div y \rfloor \)

Equivalence classes (mod as an equivalence relation)
- \( a \equiv b \mod m \) if \( a - b \) is a multiple of m

Residue classes mod m
- \( m \) of them
  - All a such that \( a \equiv 0 \mod m \)
  - All a such that \( a \equiv 1 \mod m \)
  - ...  
  - All a such that \( a \equiv m-1 \mod m \)

Modulo Arithmetic

If:
- \( x = x' \mod m \)
- \( y = y' \mod m \)

Then
- \( x + y \equiv x' + y' \mod m \)
- \( x - y \equiv x' - y' \mod m \)
- \( xy \equiv x'y' \mod m \)

Applications
- Casting out 9's

\[
\begin{align*}
532 + 656 & \equiv 327 + 55 \\
95 \times 55 & \equiv 17985 \\
\end{align*}
\]