Infinite Hierarchy of Infinities

|N| = \aleph_0
Given a 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:
  Boolean trouble(String program) {
    if not Halt(program, program) 
      return false;
    else
      while (true) ;
  }

Diagonalization (with trouble2):

Assume there exists routine:
- Boolean Halt(String program, String input) (returns true if program executed on input halts, false otherwise)
- We can write:
  Boolean trouble2(String program) {
    return not Halt(program, program);
  }
- Diagonalization (with trouble2):
**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:**

\[
\begin{align*}
\text{Floor and Ceiling} \\
\text{Ceiling(x)}: & \quad \lceil x \rceil \\
\text{Floor(x)}: & \quad \lfloor x \rfloor
\end{align*}
\]

**For real \( x \), integer \( n \):**

- \( x = n \) \( \iff \) \( n \leq x < n+1 \)
- \( x = n \) \( \iff \) \( x-1 < n \leq x \)
- \( \lceil x \rceil = n \) \( \iff \) \( n-1 < x \leq n \)
- \( \lfloor x \rfloor = n \) \( \iff \) \( x \leq n < x+1 \)

- \( \lceil x+n \rceil = \lceil x \rceil + n \)
- \( \lfloor x \rfloor = \lfloor x \rfloor \)
- \( \lfloor x \rfloor = \lfloor x \rfloor \)

**Modulo**

**Remainder when dividing two positive integers (mod as an operator):**

\[ n = m \cdot \frac{n}{m} + (n \mod m) \]

**Extended to negative numbers \( (y \neq 0) \):**

\[ x \mod y = x - y \cdot \lfloor \frac{x}{y} \rfloor \]

**Equivalence classes (mod as an equivalence relation):**

\[ a \equiv b \mod m \iff a-b \text{ is a multiple of } m \]

**Residue classes mod m**

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

**Modulo Arithmetic**

**If:**

- \( x = x' \mod m \)
- \( y = y' \mod m \)
- \( z = z' \mod m \)

**Then**

- \( x + y \equiv x' + y' \mod m \)
- \( x - y \equiv x' - y' \mod m \)
- \( xy \equiv x'y' \mod m \)
- \( xy+z \equiv x'y' +z' \mod m \)
Casting out 9's

Given x, how to calculate $x \mod 9$

- Take all the digits of x
- Add them together. If the result is bigger than 9, use this formula recursively

**Shortcut:**

- As you are adding the digits of x, if you ever have an intermediate value ≥ 9, add its two digits together
- If you ever find a 9, throw it away (cast it out)

**Casting out 9's**

\[\begin{array}{c}
532 \\
+ 656 \\
95 \\
\hline
1273
\end{array}\]

\[\begin{array}{c}
5723386 \\
x \\
51553 \\
\hline
295057718458
\end{array}\]

**Why it works:**

- $10 \equiv 1 \mod 9$
- $10^n \equiv 1 \mod 9$
- $10^n a \equiv a \mod 9$
- $10^n a + 10^{n-1} b + 10^{n-2} c + \ldots + 10 y + z \equiv (a + b + c + \ldots + y + z) \mod 9$

**Limitations:**

- $9$

Rationals and Irrationals

Rationals are closed under addition, subtraction, multiplication, and division

- except division by zero

Irrationals are **not** closed under multiplication

- Irrational * rational may equal rational

- What about irrational * (non-zero) rational?

Casting out 11's

Given x, how to calculate $x \mod 11$

- Starting from the right, alternately add and subtract each digit

\[\begin{array}{c}
532 \\
+ 656 \\
95 \\
\hline
1823
\end{array}\]

\[\begin{array}{c}
5723386 \\
x \\
51553 \\
\hline
259057718458
\end{array}\]

**Why it works:**

- $10 \equiv -1 \mod 11$
- $100 \equiv (10 \times 10) \mod 11 \equiv (-1 \times -1) \mod 11 = 1 \mod 11$
- if $n$ is even: $10^n \equiv 1 \mod 1$
- odd: $10^n \equiv -1 \mod 1$
- $10^n a \equiv a \mod 11$ (or $10^n a \equiv -a \mod 11$)
- $10^n a + 10^{n-1} b + 10^{n-2} c + \ldots + 10 y + z \equiv (z + -1 y + \ldots + -1 c + 1 b + -1 b) \mod 11$
- $(z - y + \ldots -c + b - a) \mod 11$

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 $2^{m+1} = 2m + 2^{m-1} = 2^{m-2} + \ldots + 1$
- 43rd known Mersenne prime: $2^{20,402,457} - 1$
- Contains >9,000,000 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

Distribution of Prime Numbers

- There are approximately $x/\ln x$ primes $\leq x$
- (The size of the $n$th prime is approximately $n/\ln n$)