

CSE 20—Discrete Math

Fall, 2005

October 11 (Day 6)
Number Theory

Instructor: Neil Rhodes

Rationals are Countable

2

Reals are not Countable

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

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

Diagonalization Argument

3

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

4

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 Halt(program, program)
        return false;
    else
        while (true) ;
}
```
- Diagonalization:

5

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?

6

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 $2^{km} - 1 = (2^m - 1)(2^{m(k-1)} + 2^{m(k-2)} + \dots + 1)$
- 38th known Mersenne prime: $2^{6,972,593} - 1$
 - Contains >2,000,000 digits

7

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

8

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:

9

Floor and Ceiling

$\lceil x \rceil = x \leftrightarrow x \text{ is an integer} \leftrightarrow \lfloor x \rfloor = x$

$$x-1 < \lfloor x \rfloor \leq x \leq \lceil x \rceil < x+1$$

For real x, integer n:

- $\lfloor x \rfloor = n \leftrightarrow n \leq x < n+1$
- $\lfloor x \rfloor = n \leftrightarrow x-1 < n \leq x$
- $\lceil x \rceil = n \leftrightarrow n-1 < x \leq n$
- $\lceil x \rceil = n \leftrightarrow x \leq n < x+1$

- $\lceil x+n \rceil = \lceil x \rceil + n$
- $\lfloor -x \rfloor = -\lceil x \rceil$
- $\lceil -x \rceil = -\lfloor x \rfloor$

10

Modulo

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

- $n = m \lfloor n/m \rfloor + (n \bmod m)$

Extended to negative numbers ($y \neq 0$)

- $x \bmod y = x - y \lfloor x/y \rfloor$

Equivalence classes (mod as an equivalence relation)

- $a \equiv b \bmod m$ iff a-b is a multiple of m

Residue classes mod m

- m of them
 - All a such that $a \equiv 0 \bmod m$
 - All a such that $a \equiv 1 \bmod m$
 - ...
 - All a such that $a \equiv m-1 \bmod m$

11

Modulo Arithmetic

If:

- $x \equiv x' \bmod m$
- $y \equiv y' \bmod m$

Then

- $x + y \equiv x' + y' \bmod m$
- $x - y \equiv x' - y' \bmod m$
- $xy \equiv x'y' \bmod m$

Applications

- Casting out 9's

$$\begin{array}{r} 532 \\ + 656 \\ 95 \\ \hline 1273 \end{array}$$

$$\begin{array}{r} 327 \\ \times 55 \\ \hline 17985 \end{array}$$

12