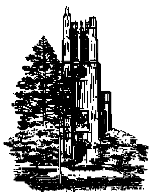
Thursday June 9, 2016
Lecture 15

Number Theory



Notables

- Reach Chapter 4
- Homework #9
  - Page 229, Problems 2, and 16
  - Page 244, Problems 6, 10, and 14,
  - Page 245, Problems 28, and 32
    - Due, Tuesday June 14, 2016

Complexity of Algorithms

TABLE 1 Commonly Used Terminology for the Complexity of Algorithms.

Complexity	*Terminology*
$\Theta(1)$	Constant complexity
$\Theta(\log n)$	Logarithmic complexity
$\Theta(n)$	Linear complexity
$\Theta(n \log n)$	Linearithmic complexity
$\Theta(n^b)$	Polynomial complexity
$\Theta(b^n)$, where $b > 1$	Exponential complexity
$\Theta(n!)$	Factorial complexity

Complexity of Algorithms…

TABLE 2 The Computer Time Used by Algorithms.

Problem Size	*Bit Operations Used*					
n	$\log n$	n	$n \log n$	n^2	2^n	$n!$
10	3×10^{-11} s	10^{-10} s	3×10^{-10} s	10^{-9} s	10^{-8} s	3×10^{-7} s
10^2	7×10^{-11} s	10^{-9} s	7×10^{-9} s	10^{-7} s	4×10^{11} yr	*
10^3	1.0×10^{-10} s	10^{-8} s	1×10^{-7} s	10^{-5} s	*	*
10^4	1.3×10^{-10} s	10^{-7} s	1×10^{-6} s	10^{-3} s	*	*
10^5	1.7×10^{-10} s	10^{-6} s	2×10^{-5} s	0.1 s	*	*
10^6	2×10^{-10} s	10^{-5} s	2×10^{-4} s	0.17 min	*	*

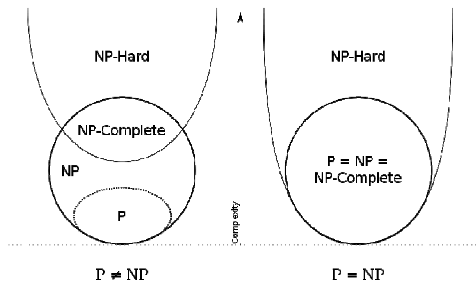
Complexity of Decision Problems

- *Tractable Problem*: There exists a polynomial time algorithm to solve this problem. These problems are said to belong to the *Class P*.
- *Intractable Problem*: There does not exist a polynomial time algorithm to solve this problem
- *Unsolvable Problem* : No algorithm exists to solve this problem, e.g., halting problem.
- *Class NP*: Solution can be checked in polynomial time. But no polynomial time algorithm has been found for finding a solution to ALL problems in this class. Note that a problem in *Class P* is also in *Class NP*
- *NP Complete Class*: If you find a polynomial time algorithm for one member of the class, it can be used to solve all the problems in the class.

P versus NP challenge

- The *P versus NP problem* asks whether the class P = NP? Are there problems whose solutions can be checked in polynomial time, but can not be solved in polynomial time?
  - Note that just because no one has found a polynomial time algorithm is different from showing that the problem can not be solved by a polynomial time algorithm.
- If a polynomial time algorithm for any of the problems in the NP complete class were found, then that algorithm could be used to obtain a polynomial time algorithm for every problem in the NP class.
  - Satisfiability (in Section 1.3) is an NP complete problem.
- It is generally believed that P≠NP since no one has been able to find a polynomial time algorithm for any of the problems in the NP complete class.
- The problem of P versus NP remains one of the most famous unsolved problems in mathematics (including theoretical computer science). The Clay Mathematics Institute has offered a prize of $1,000,000 for a solution.

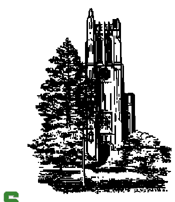
A simple view of complexity classes



450

Number Theory

Chapter 4



451

Outline

- Division: Factors, multiples
- Primes: The Fundamental Theorem of Arithmetic.
- The Division Algorithm
- Greatest Common Divisors: Relatively prime
- Least Common Multiples
- Modular Arithmetic: Congruence
- Applications of Congruence

452

Division (review)

- Let a be an integer and m a positive integer. Then there are *unique* integers q and r, with $0 \le r < m$, such that $a = dq + r$
  - a is called the *dividend*,
  - m is called the *divisor*,
  - q is called the *quotient*, $q = a \text{ div } d = \lfloor a/d \rfloor$
  - r is called the *reminder*, $r = a \bmod d$

453

Division

- Definition: Let a and b be integers with $a \neq 0$. Then, we say that a *divides* b, denoted $a \mid b$, if there is an integer c such that $b = ac$.
  - a is called a *factor* of b, and b is a *multiple* of a.
  - We denote $a \nmid b$ when a does not divide b
  - $a \mid b$ is equivalent to $\exists c\ (b = ac)$ where the universe of discourse is $\mathbf{Z}$.

454

Division Facts

- Theorem: Let a, b, c be integers with $a \neq 0$. Then,
  - if $a \mid b$ and $a \mid c$ then $a \mid (b + c)$
  - if $a \mid b$ then $a \mid bc$
  - if $a \mid b$, and $b \mid c$ then $a \mid c$.
  - If $a \mid b$ and $a \mid c$ then $a \mid (mb + nc)$ whenever m and n are integers.

455

Primes

- Definition: A positive integer $p > 1$ is called *prime* if the only positive factors of p are 1 and p.
  - A positive integer that is greater than 1 and is not prime is called *composite*.
  - Note that number 1 is neither prime nor composite.
  - Some primes: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47…
  - How many digits in the largest prime found to-date (2016)?
    - 22,338,618 digits
    - A Mersenne prime = $2^{74,207,281} - 1$

456

Prime Theorems

- Theorem 1: Every positive integer $n > 1$ has a prime factor $\leq n$. Why?
- Theorem 2: Every positive integer $n > 1$ can be written *uniquely* as a prime or as the product of primes, in non-decreasing order. (proof later)
- Theorem 3: If n is a composite integer, then n has a prime factor $\leq \sqrt{n}$. Why?
- Corollary: If n does not have a prime factor $\leq \sqrt{n}$ then it is prime. Why?
- Conjecture: Every even integer > 2 can be written as the sum of two primes.

457