Announcements

- Second HW due today
- Quiz 1 is on Wednesday, here, first 15 minutes of class

http://www.cs.uiuc.edu/class/sp10/cs173

Number Theory

- A branch of mathematics focused on integers

- Very important applications in:
  - Cryptography
  - Randomized algorithms and data-structures (e.g., hash tables)
  - Acoustics

- **Definition**: $a \in \mathbf{Z}$ divides $b \in \mathbf{Z}$ if $\exists n \in \mathbf{Z}$, $b = a.n$
  - Notation: $a \mid b$
  - a is a factor of b
  - b is a multiple of a

- *Examples*: $-7 \mid 77$, because $77 = (-11)(-7)$ and $-11 \in \mathbf{Z}$
  $7 \mid 0$, because $0 = 0 \times 7$ and $0 \in \mathbf{Z}$

- Does $0 \mid 7$? Does $0 \mid 0$?

Direct proof with divisibility

- $\forall a, b, c \in \mathbf{Z}, \quad a \mid b \;\wedge\; a \mid c \;\rightarrow\; a \mid (b + c)$

- **Proof**: Suppose a, b and c are integers such that $a \mid b$ and $a \mid c$

  Then, by definition, $\exists n \in \mathbf{Z},\; b = an$
  and $\exists m \in \mathbf{Z},\; c = am$

  Hence, $b + c$
  $= (an + am)$
  $= a(n + m)$, where $(n + m) \in \mathbf{Z}$

  Hence, $a \mid (b + c)$

- Similarly: $\forall a, b, c \in \mathbf{Z}, \quad a \mid b \;\rightarrow\; a \mid bc$
  $\forall a, b, c \in \mathbf{Z}, \quad a \mid b \;\wedge\; b \mid c \;\rightarrow\; a \mid c$ (transitivity)

Prime Numbers

- **Definition**: An integer $p \geq 2$ is prime if the only positive factors of p are 1 and p

  $\forall p \in \mathbf{Z},\ p$ is prime $\leftrightarrow p \geq 2 \ \wedge$

  $\forall q \in \mathbf{Z},\ (q > 0) \wedge (q \mid p) \ \rightarrow\ (q = 1) \vee (q = p)$

- **Definition**: An integer $c \geq 2$ is composite if c is not prime

- **Fundamental Theorem of Arithmetic (FTA)**: Every integer $n \geq 2$ can be written as a product of one or more prime factors. This prime factorization is *unique* (except for the order of the prime factors).

  Examples: $260 = 2 \times 2 \times 5 \times 13$ and $17 = 17$

- There are fast algorithms for testing whether a number is prime

- Algorithms for finding factors of composite numbers are slow
  - Basis for cryptography (RSA)

GCD and LCM

- If $c \mid a$ and $c \mid b$ then c is a common divisor of a and b
- The greatest common divisor of a and b = gcd(a, b) is the largest common divisor of a and b
- Similarly if $a \mid c$ and $b \mid c$ then c is a common multiple of a and b
- The least common multiple of a and b = lcm(a, b) is the smallest common multiple of a and b
- Integers a and b are relatively prime if gcd(a, b) = 1

$$lcm(a,b) = \frac{ab}{\gcd(a,b)}$$

- Next week: A fast algorithm for computing gcd(a, b)

There are infinitely many prime numbers

- **Euclid's Theorem (300 BC)**: There are infinitely many prime numbers

- **Proof by contradiction**: Suppose there are only finitely many primes

  Let's list them all: $p_1,\ p_2,\ p_3,\ \ldots,\ p_n$

  Let $q = 1 + \prod_{i=1}^{n} p_i$

  By the FTA, q must have a prime factor

  However, none of the prime numbers in our list divides q because they all leave remainder 1

  So $p_1,\ p_2,\ p_3,\ \ldots,\ p_n$ cannot be a list of *all* prime numbers, a contradiction!