Mathematics Review

- Exponents:

$$X^A X^B = X^{A+B}$$

$$X^A / X^B = X^{A-B}$$

$$(X^A)^B = X^{AB}$$

$$X^N + X^N = 2X^N$$

$$2^N + 2^N = 2^{N+1}$$

Logarithms

- Definition:

  $X^A = B$ iff $\log_X B = A$
- Useful formulas:

  $\log_A B = (\log_C B) / (\log_C A)$, $A, B, C > 0$ and $A \neq 1$

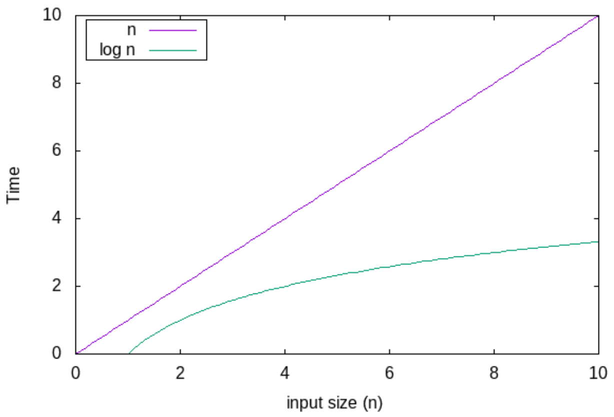
  $\log AB = \log A + \log B$, $A, B > 0$

  $\log A/B = \log A - \log B$

  $\log (A^B) = B \log A$

  $\log 1 = 0$, $\log 2 = 1$

  $\log X < X$ for all $X > 0$



- Unless specified otherwise, all log are base 2.

Series

$$\sum_{i=0}^{N} 2^i = 2^{N+1} - 1$$

$$\sum_{i=0}^{N} A^i = \frac{A^{N+1} - 1}{A - 1}$$

If $0 < A < 1 \Rightarrow \quad \sum_{i=0}^{N} A^i \leq \frac{1}{1-A}$

$$\sum_{i=0}^{\infty} A^i = \frac{1}{1-A}$$

$$\sum_{i=0}^{\infty} \frac{i}{2^i} = 2$$

Series

$$\sum_{i=1}^{N} i = \frac{N(N+1)}{2} \approx \frac{N^2}{2}$$

$$\sum_{i=1}^{N} i^2 = \frac{N(N+1)(2\mathrm{N}+1)}{6} \approx \frac{N^3}{3}$$

$$\sum_{i=1}^{N} i^k \approx \frac{N^{k+1}}{|k+1|}$$

$$H_N = \sum_{i=1}^{N} \frac{1}{i} \approx \log_e N \qquad e = 2.71828\ldots$$

Modular Arithmetic

- Definition:

  $A \equiv B \pmod{N}$ if N divides A-B

  i.e. the remainder is the same when either

  A or B is divided by N.

- Example:

  $81 \equiv 61 \equiv 1 \pmod{10}$

- If $A \equiv B \pmod{N}$ then

  $A+C \equiv B+C \pmod{N}$ and $AD \equiv BD \pmod{N}$

Proofs

- By Induction
- By Counterexample
- By Contradiction

Proof by Induction

- Historical notes:
  - first known proof by induction, Francesco Maurolico in 1575
  - Fermat, 17th century called it “the method of infinite descent”
  - “mathematical induction” coined by A. de Morgan, early 19th century
- Proof by Induction:

  1. Proving the Base Case:

     Establish that a theorem is true for some small values.

  2. Inductive Hypothesis:

     Assume an inductive hypothesis, e.g. assume that the theorem is true for all cases up to some value k.

     Show that the theorem is true for the next value (typically k+1)

     Note: It works as long as k is finite!

     It can be viewed as an algorithmic proof procedure!

Proof by Induction: Example

- Problem:

  Prove that Fibonacci numbers,

  $F_0 = 1, F_1 = 1, F_2 = 2, F_3 = 3, F_4 = 5, \ldots,$

  $F_i = F_{i-1} + F_{i-2}$ satisfy $F_i < (5/3)^i$

- Base case: verify that

  $F_1 = 1 < 5/3$ and $F_2 = 2 < 25/9$

- Inductive Hypothesis:

Assume that $F_i < (5/3)^i$ is true for $i = 1, 2, \ldots, k$

We need to show that $F_{k+1} < (5/3)^{k+1}$

Historical note: Fibonacci sequence introduced in Fibonacci's book "Liber Abaci", 1202.

Proof by Induction: Example

$F_{k+1} = F_k + F_{k-1}$

$F_{k+1} < (5/3)^k + (5/3)^{k-1}$

$= (3/5)(5/3)^{k+1} + (3/5)^2(5/3)^{k+1}$

$= (3/5)(5/3)^{k+1} + (9/25)(5/3)^{k+1}$

$= (3/5 + 9/25)\ (5/3)^{k+1}$

$= (24/25)(5/3)^{k+1}$

$< (5/3)^{k+1}$ => The theorem is proved

Proof by Counterexample

- The statement $F_k \leq k^2$ is false.
- Compute $F_{11} = 144 > 11^2$

Proof by Contradiction

- Technique:

  assume that the theorem is false and show that this assumption implies that some known property is false.
- Example:

  There is an infinite number of primes.

  (Euclid, ~ 300 BC)

- Assume that the theorem is false i.e. there is some largest prime P_k.
- Consider $N = P_1 P_2 P_3 \ldots P_k + 1$, P_i ordered primes
- Clearly N is larger than P_k => by assumption N is not prime!
- None of the P_i divides N exactly (remainder =1)

=> Contradiction: every number is either prime or a product of primes.