

1 Exponents

$$\begin{aligned}X^A X^B &= X^{A+B} \\ \frac{X^A}{X^B} &= X^{A-B} \\ (X^A)^B &= X^{AB} \\ X^N + X^N &= 2X^N \neq X^{2N} \\ 2^N + 2^N &= 2^{N+1}\end{aligned}$$

2 Logarithm

$$\begin{aligned}X^A = B &\Leftrightarrow \log_X B = A \\ \log_A B &= \frac{\log_C B}{\log_C A} \\ \log AB &= \log A + \log B \\ \frac{\log A}{\log B} &= \log A - \log B \\ \log(A^B) &= B \log A \\ \log X < X &\text{ for all } X > 0\end{aligned}$$

3 Series

$$\begin{aligned}\sum_{i=0}^N 2^i &= 2^{N+1} - 1 \\ \sum_{i=0}^N A^i &= \frac{A^{N+1} - 1}{A - 1} \\ \sum_{i=0}^N A^i &\leq \frac{1}{1 - A} \quad \text{if } 0 < A < 1, \quad N \rightarrow \infty\end{aligned}$$

3.1 Proof for $\sum_{i=0}^{infy}$

$$S = \sum_{i=0}^N = 1 + A + A^2 + A^3 + \cdots + A^{N-1} + A^{N+1}$$

then

$$AS = A + A^2 + A^3 + A^4 + \cdots + A^N + A^{N+1}$$

then

$$AS = S - 1 + A^{N+1}(1)$$

then

$$S = \frac{A^{N+1} - 1}{A - 1}$$

if $0 < A < 1$ then $A^{N+1} \rightarrow 0, N \rightarrow \infty$ then

$$(1) \Leftrightarrow AS = S - 1 \Leftrightarrow S = \frac{1}{1 - A}$$

3.2 Proof for $\sum_{i=1}^{\infty} i/2^i$

Suppose

$$S = \sum_{i=1}^N i/2^i = \frac{1}{2} + \frac{2}{2^2} + \frac{3}{2^3} + \frac{4}{2^4} + \cdots + \frac{N-1}{2^{N-1}} + \frac{N}{2^N}$$

then

$$2S = 1 + \frac{2}{2} + \frac{3}{2^2} + \frac{4}{2^3} + \frac{5}{2^4} + \cdots + \frac{N}{2^{N-1}}$$

then

$$2S - S = 1 + \frac{1}{2} + \frac{1}{2^2} + \frac{1}{2^3} + \frac{1}{2^4} + \cdots + \frac{1}{2^{N-1}} + \frac{N}{2^N}$$

Since $\lim_{N \rightarrow \infty} \frac{N}{2^N} = \lim_{N \rightarrow \infty} \frac{1}{2^N \ln 2} = 0$, then

$$S = 1 + \frac{1}{2} + \frac{1}{2^2} + \frac{1}{2^3} + \frac{1}{2^4} + \cdots + \frac{1}{2^{N-1}}$$

Or

$$S = \sum_{i=0}^{N-1} (1/2)^i = \sum_{i=0}^{\infty} (1/2)^i = \frac{1}{1 - 1/2} = 2$$

3.3 Arithmetic series

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

$$2 + 5 + 8 + \cdots + (3k-1) = 3(1 + 2 + 3 + \cdots + k) - (1 + 1 + \cdots + 1) = \frac{3k(k+1)}{2} - k$$

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

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

If, $k = -1$, the sum is then the harmonic number H_N

$$H_N = \sum_{i=1}^N \frac{1}{i} \approx \log_{\epsilon} N$$

with error tends to $\gamma = 0.57721566$, also known as **Euler's constant**

$$\sum_{i=1}^N f(N) = Nf(N)$$

$$\sum_{i=n_o}^N f(i) = \sum_{i=1}^N f(i) - \sum_{i=1}^{n_o-1} f(i)$$

4 Modular Arithmetic

- A is congruent to B modulo N , written $A \equiv B \pmod{N}$, if N divides $A - B$.
- Intuitively, the remainder is the same when either A or B is divided by N .

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

$$A + C \equiv B + C \pmod{N}$$

$$AD \equiv BD \pmod{N}$$

If N is a prime number:

- $ab \equiv 0 \pmod{N} \Leftrightarrow a \equiv 0 \pmod{N} \text{ or } b \equiv 0 \pmod{N}$. In other words, if a prime number N divides a product of two numbers, it divides at least one of the two numbers.
- $ax \equiv 1 \pmod{N}$ has a unique solution $x \pmod{N}$ for all $0 < a < N$. This solution, $0 < x < N$, is the multiplicative inverse.
- The equation $x^2 \equiv a \pmod{N}$ has either two solutions for all $0 < a < N$, or it has no solution.

5 The P Word

5.1 Proof by induction

- Proving a base case that is establishing that a theorem is true.
- Assuming an inductive hypothesis that is true for all case. Showing that the theorem is true for the next value, $k + 1$.

5.2 Proof by Counterexample

Find something that counter the statements

5.3 Proof by contradiction