Modern Cryptography

Logs and exponents: Notes on September 3, 2021

Jeffrey Goldberg
jeffrey@goldmark.org

August 27, 2021
Revised May 8, 2024

Logarithms

Inverse of exponetiation

if $y = 10^x$ then $x = \log_{10} y$. This is read as “x is the (base 10) logarithm of y.

Example 1 (Powers of 10 & $\log_{10}$)

$$\begin{aligned} 100 = 10^2, &\quad 2 = \log_{10}(100) \\ 10 = 10^1, &\quad 1 = \log_{10}(10) \\ 1 = 10^0, &\quad 0 = \log_{10}(1) \\ 1/10 = 10^{-1}, &\quad -1 = \log_{10}(0.1) \\ 1/100 = 10^{-2}, &\quad -2 = \log_{10}(0.01) \end{aligned}$$

Properties of exponentiation

Integer exponents: Definitions

Definition 2 (Integer exponents)

$$b^n = \begin{cases} 1 & \text{when } n = 0 \\ b \cdot b^{n-1} & \text{otherwise} \end{cases}$$

Definition 3 (Also integer exponents)

$$b^n = \begin{cases} 1 & \text{when } n = 0 \\ \frac{b^{n+1}}{b} & \text{otherwise} \end{cases}$$

Those two definitions are equivalent, but the first is easier to use when $n > 0$ and the second is easier to use when $n < 0$.

Integer exponents: Definitions

Definition 2 (Integer exponents)

$$b^n = \begin{cases} 1 & \text{when } n = 0 \\ b \cdot b^{n-1} & \text{otherwise} \end{cases}$$

Definition 3 (Also integer exponents)

$$b^n = \begin{cases} 1 & \text{when } n = 0 \\ \frac{b^{n+1}}{b} & \text{otherwise} \end{cases}$$

Those two definitions are equivalent, but the first is easier to use when $n > 0$ and the second is easier to use when $n < 0$.

You can't understand properties of logarithms without understanding properties of exponentiation.

Example 4

Using definition With $b = 10$

$$
\begin{aligned}
10^0 &= 1 \\
10^1 &= 10 \cdot 10^0 = 10 \cdot 1 = 10 \\
10^2 &= 10 \cdot 10^1 = 10 \cdot 10 = 100 \\
10^{-1} &= 10^0/10 = 1/10 = 0.1 \\
10^{-2} &= 10^{-1}/10 = 0.1/10 = 0.01
\end{aligned}
$$

Properties of exponentiation

Addition	$b^n b^m$	$= b^{n+m}$
Subtraction	$\frac{b^n}{b^m}$	$= b^{n-m}$
Multiplication	$b^{n^m} = (b^n)^m$	$= b^{mn}$

Table 1: What we do in the exponents: We add exponents instead of multiplication the base realm.

Recalling that $b^n b^m = b^{n+m}$ we wish so solve for x in $2^x 2^x = 2$.

$$2^1 = 2^x 2^x = 2^{x+x}$$
$$1 = x + x$$
$$x = 1/2$$
$$2 = (2^{\frac{1}{2}})(2^{\frac{1}{2}})$$
$$2^{\frac{1}{2}} = \sqrt{2}$$

In general $b^{\frac{1}{n}} = \sqrt[n]{b}$ and $b^{\frac{m}{n}} = b^m \sqrt[n]{b}$.

Logarithms are exponents. So what we can do with exponents we can do with logs.

Base realm	Exponential realm	Example
xy	$\log(x) + \log(y)$	$100 \cdot 1000 = b^{\log_b(100)+\log_b(1000)}$
x/y	$\log(x) - \log(y)$	$100/1000 = b^{\log_b(100)-\log_b(1000)}$
x^y	$y\log(x)$	$10^3 = b^{3\log_b(10)}$

Table 2: Properties of logarithms: Logs turn multiplication into addition, division into subtraction, and exponentiation into multiplications.

Properties of logs: Examples with $b = 10$

$$
\begin{aligned}
100 \cdot 1000 &= 10^{\log_{10}(100)+\log_{10}(1000)} &&= 10^{2+3} &&= 10^5 &&= 100000 \\
100/1000 &= 10^{\log_{10}(100)-\log_{10}(1000)} &&= 10^{2-3} &&= 10^{-1} &&= 0.1 \\
10^3 &= 10^{3\log_{10}(10)} &&= 10^{3\cdot 1} &&= 10^3 &&= 1000
\end{aligned}
$$

Properties of logs: Examples with $b = 2$

$$
\begin{aligned}
100 \cdot 1000 &= 2^{\log_2(100)+\log_2(1000)} &\approx 2^{6.64+9.97} &\approx 2^{16.61} &= 100000 \\
100/1000 &= 2^{\log_2(100)-\log_2(1000)} &\approx 2^{6.64-9.97} &\approx 2^{3.32} &= 0.1 \\
10^3 &= 2^{3\log_2(10)} &= 2^{3\cdot 3.32} &\approx 2^{9.67} &= 1000
\end{aligned}
$$

Notation

We will use "$\log$" to mean either base 2 logarithms or when we don't care about that base. We will use "$\ln$" for the natural logarithm.

base	*explicit*	*school*	*math/physics*	*crypto*
10	$\log_{10}$	$\log$	$\log_{10}$	$\log_{10}$
e	$\log_e$	$\ln$	$\log, \ln$	$\ln$
2	$\log_2$	$\log_2$	$\lg$	$\log$
Don't care	$\log$	$\log$	$\log$	$\log$

Table 3: What "$\log$" means to whom. In US high schools it typically is used for base 10. Elsewhere it is for the natural logarithm. In cryptography and information theory it is typically base 2.