

Teaching logarithms in the algebra classroom and understanding them at a new level.

Autumn Malloy

California Lutheran University

May 9th, 2007

The Main Point

- To gain insight into teaching: Is this the career path I want to choose?
- To develop a way to teach logarithms that is more understandable and that shows their connection to something other than themselves.
- To understand discrete logarithms and their connection to continuous logarithms.

- California State Standards
 - 11.0 Students prove simple laws of logarithms.
 - 11.1 Students understand the inverse relationship between exponents and logarithms and use this relationship to solve problems involving logarithms and exponents.
 - 11.2 Students judge the validity of an argument according to whether the properties of real numbers, exponents, and logarithms have been applied correctly at each step.

- History

- John Napier was the first published; 1614 in Scotland
- used $1/e$ as the base to make some difficult calculations possible
- used in astronomy, surveying, navigation, computing products and more before calculators and computers

- Applications

- compound interest
- exponential growth and decay
- earthquake intensity (Richter scale)

- Lesson Plan
 - I have created and taught a lesson plan covering:
 - review of the rules of exponents
 - logarithm definition and relationship to exponents
 - expressing logarithmic functions as exponential functions, and vice versa
 - evaluating logarithms
 - deriving the properties of logarithms from the rules of exponents
 - I have also created a review sheet on exponential functions and a worksheet for use as an assessment tool.

- Lesson Plan Review
 - student participation was decent
 - All of the students stated that this lesson plan helped clear up some confusion about logarithms.
 - specific mention to where each number went (log BOP)
 - average score was 77%
 - problems with understanding the power rule, computation, knowing which rule to apply
 - Overall, this was a good first experience with teaching. I look forward to getting back into the classroom in the future.

Discrete Logarithms

- primitive root
 - r =primitive root of n where $r^{\phi(n)} \equiv 1 \pmod n$
 - n only has a primitive root if $n= 2, 4,$ odd prime $p, p^2,$ or $2p^2$
- discrete logarithm
 - n =integer, r =primitive root, a =positive integer
 - $(a, n) = 1, x$ =integer where $1 \leq x \leq \phi(n)$ and $r^x \equiv a \pmod n$
 - x is the index, or discrete logarithm, of a to the base $r \pmod n$
 - $\rightarrow a \equiv r^{\text{ind}_r a} \pmod n$

Discrete Logarithms

- Discrete logarithm problem: given prime p , and primitive root r , finding $r^{\text{ind}_r a} \equiv a \pmod{p}$ is very difficult. It is said to be as difficult as factoring integers into prime numbers. This serves as the base for applications of discrete logarithms within cryptography.
- ElGamal Cryptosystem: public key cryptography

How it works:

- Public key: (p, r, b) ; Private key: a
- p =prime, r =primitive root of p , a =integer where $0 \leq a \leq p - 1$
- b =integer where $b \equiv r^a \pmod{p}$

- ElGamal Cryptosystem

- 1 The recipient (R) creates the public and private keys and sends the public key to the sender (S).
- 2 S translates the original message into numerical form. This message is then broken into smaller, even numbered parts m_1, m_2, \dots, m_i .
- 3 For each m_i , S chooses a random integer k ($1 \leq k \leq p - 2$) and computes $\gamma \equiv r^k \pmod{p}$ where $0 \leq \gamma \leq p - 1$ and $\delta \equiv m_i * b^k \pmod{p}$ where $0 \leq \delta \leq p - 1$
- 4 S sends $E(m_i) = (\gamma, \delta)$ to R.
- 5 R computes $\gamma^{p-1-a} * \delta \pmod{p}$ using the private key, a .
- 6 This number is m_i , which R translates back into alphabetical form.
- 7 Repeat steps 3-6 for each m_i , to compile the full, original message

Discrete logarithms have similar properties to continuous logarithms:

- $\log_b 1 = 0$
 $ind_r 1 \equiv 0 \pmod{\phi(m)}$
- Product: $\log_b x * y = \log_b x + \log_b y$
 $ind_r x * y \equiv (ind_r x + ind_r y) \pmod{\phi(m)}$
- Power: $\log_b x^k = k \log_b x$
 $ind_r x^k \equiv k ind_r x \pmod{\phi(m)}$

Discrete logarithms have a close relationship to the order of an integer. Algebraic logarithms have an inverse relationship with exponents.

- In Number Theory, discrete logarithms are presented as a close form of the order of an integer. This helps relate the topic to material that is already learned
- In Algebra, however, logarithms are often presented as a new, separate topic. If they would instead be explained as a form of exponential functions (inverse form), they would not seem like such an unfamiliar concept to many students

Now That It's Over

- I have discovered that I still want to pursue teaching high school math, but not immediately.
- I believe that I have a lesson plan that is understandable to and reaches students at different levels.
- I have developed a better understanding of how studying higher level math can benefit teaching math in secondary schools.

Bibliography

- Martin-Gay, K. Elayn. Intermediate Algebra. Fourth Edition. Upper Saddle River, New Jersey: Pearson Education, Inc., 2005.
- Menezes, A.J., van Oorschot, P.C., Vanstone, S.A. Handbook of Applied Cryptography. Boca Raton, Florida: CRC Press, 1997.
- Rosen, Kenneth H. Elementary Number Theory. Fourth Edition. Reading, Massachusetts: AT T Laboratories, 2000.
- Rudin, Walter. Principles of Mathematical Analysis. Third Edition. Tokyo: McGraw-Hill Kogakusha, Ltd, 1976.
- “Algebra II Mathematics Content Standards.” California State Board of Education . 08 Mar 2006. 01 Nov 2006
[<http://www.cde.ca.gov/be/st/ss/mthalgebra2.asp>].
- Professor Dorff, Dr. Fogel, Dr. McCambridge, Dr. Soderlund