Math 348 reqd. Spring 2022

Intro to Discrete Logs

simplifies

1. For positive real numbers a and b with $b > 1$, what does $\log_b(a)$ mean?

$\log_b(a)$ is the power you have to raise b to in order to get a.

requires pf. $\longrightarrow$ $\exists !\, x : b^x = a$

Define $\log_b(a) = x$

2. The goal for this section is to come up with a good definition for $\log_b(a) \bmod m$. We'll start by doing an example. Recall that we have the following table of powers for $(\mathbb{Z}/9\mathbb{Z})^\times$:

x	1	2	3	4	5	6	7	8	9	10	11	12
1^x	1	1	1	1	1	1						
2^x	2	4	8	7	5	1	2	4	8	7	5	1
4^x	4	7	1	4	7	1						
5^x	5	7	8	4	2	1						
7^x	7	4	1	7	4	1						
8^x	8	1	8	1	8	1						

When working mod 9...

(a) What should $\log_2(2)$ be?

The power of 2 that yields 2

$2^x \equiv 2 \bmod 9 \leftarrow x = 1$

(b) What should $\log_2(4)$ be?

$2^x \equiv 4 \bmod 9 \leftarrow x = 2$

(c) What should $\log_2(8)$ be?

$2^x \equiv 8 \bmod 9 \leftarrow x = 3$

(d) What should $\log_2(7)$ be?

$2^x \equiv 7 \bmod 9 \leftarrow x = 4$

(e) Can you come up with another reasonable answer to the previous question? What about a third answer? A fourth?

$x = 4, 10, 16, 22, \ldots$

$\hookrightarrow 2^x \equiv 7 \mod 9$

$$x \equiv 4 \mod \underset{\underset{\varphi(9)}{\parallel}}{6}$$

(f) Can you give a well-defined function $\log_2(n)$ for all $n \in (\mathbb{Z}/9\mathbb{Z})^\times$? If not, can you give a well-defined function $\log_2(n)$ up to some modulus?

n	1	2	4	5	7	8
$\log_2(n)$	0 or 6 mod 6	1 mod 6	2 mod 6	5 mod 6	4 mod 6	3 mod 6

(g) What should $\log_5(1)$ be?

(h) What should $\log_5(5)$ be?

(i) What should $\log_5(7)$ be?

(j) Can you give a well-defined function $\log_5(n)$ for all $n \in (\mathbb{Z}\,/\,9\mathbb{Z})^\times$? If not, can you give a well-defined function $\log_5(n)$ up to some modulus?

(k) What should $\log_7(7)$ be?

1

(l) What should $\log_7(4)$ be?

2

(m) What should $\log_7(5)$ be?

? no soln: $7^x \equiv 5 \mod 9$

(n) Can you give a well-defined function $\log_{\cancel{5}7}(n)$ for all $n \in (\mathbb{Z}/9\mathbb{Z})^\times$? If not, can you give a well-defined function $\log_{\underset{7}{\cancel{5}}}(n)$ up to some modulus?

No

3. Here's another example. Recall that we have the following table of powers for $(\mathbb{Z}\,/\,8\mathbb{Z})^{\times}$

x	1	2	3	4
1^x	1	1	1	1
3^x	3	1	3	1
5^x	5	1	5	1
7^x	~~5~~ 7	1	~~5~~ 7	1

Does there exist a base b so that $\log_b(n)$ is a well-defined function on $(\mathbb{Z}\,/\,8\mathbb{Z})^{\times}$ (up to some modulus)? If yes, give a table of values of $\log_b(n)$ for $n \in (\mathbb{Z}\,/\,8\mathbb{Z})^{\times}$. If no, why not?

No, b/c no prim. rt. mod 8