DLP Exercises (Daily Due Sept 14)

Katherine E. Stange, CU Boulder

In the exercises that follow, you are asked to use Sage to do computations. It's strongly recommended to use Sage instead of other software, because Sage has so many in-built number theory functions that we will make use of[1]. In particular, if Sage does something with a one-line command, and I don't specifically ask you to implement it yourself, go for it. (For example, relevant to this assignment, Sage will compute the multiplicative order of an element in an `IntegerModRing` using the command `multiplicative_order()`.)

Exercise 1

Use Sage to find all primitive roots modulo the prime 29. One of them is 2, for example.

Exercise 2

Create a chart of the powers of 2 modulo 29 (use Sage).

Exercise 3

Using the chart above, *by hand*, compute the following discrete logarithms:

1. $L_2(7)$
2. $L_2(11)$
3. $L_4(7)$ (hint: use item (1) above)

Exercise 4

1. Using Sage, but without calling any discrete logarithm functionality directly, implement an algorithm to determine the discrete logarithm of an element a modulo n with respect to a generator (primitive root) g. Paste in the code to your solutions.
2. Use the code to compute that the discrete log of 17 to the base 2 in $\mathbb{Z}/197\mathbb{Z}$ is 159, i.e. $L_2(17) = 159$ in $\mathbb{Z}/197\mathbb{Z}$. (If this doesn't work, fix your code!)

[1] But if you insist, you can use something else. I won't be able to support you with other languages/software, likely, since I'm not an expert in everything. ;)