Math 261 — Fall 2022
Number Theory

https://sites.aub.edu.lb/kmakdisi/

Problem set 5, due Friday, October 7 at the beginning of class

Exercise 5.1: a) Find all the primitive roots mod 19.

b) Find all the primitive roots mod 23.

Exercise 5.2: This exercise refers back to Exercise 3.4, and may clarify Exercise 5.1.

Assume once again that $\overline{a} \in (\mathbf{Z}/m\mathbf{Z})^*$ has multiplicative order k. Let $\ell \in \mathbf{Z}$, and take $\overline{b} = \overline{a}^\ell$. This time, do NOT suppose that $\gcd(k, \ell) = 1$.

a) Show that the order of $\overline{b}$ is exactly $k/\gcd(k, \ell)$. (Notational suggestion: write $d = \gcd(k, \ell)$, $k = dk'$, and $\ell = d\ell'$ throughout; so you want to show the order of $\overline{b}$ is k'.)

b) Now let $m = p$ be a prime number. Show that the number of primitive roots in $(\mathbf{Z}/p\mathbf{Z})^*$ is $\phi(p - 1)$.

c) Continuing with the case $m = p$, suppose $d|(p - 1)$. Show that the number of elements in $(\mathbf{Z}/p\mathbf{Z})^*$ with order d is $\phi(d)$. (The case of part (b) was when $d = p - 1$.)

d) If m is not prime, the above formulas stop working. For example, describe how many elements of each order there are in $(\mathbf{Z}/299\mathbf{Z})^*$. Please do not list all the elements! You can count the number of elements of each order by factoring $299 = (13)(23)$, and combining part (c) above with the Chinese Remainder Theorem. Think very conceptually, so as to avoid computation whenever possible.

Exercise 5.3: a) Using the fact that 3 is a primitive root mod 17, make a table of all the integers mod 17 and of their indices (i.e., discrete logarithms) with respect to 3. Indicate on your table which other elements are primitive roots mod 17.

b) Use your table to find all solutions of the following equations (all of them are mod 17):

$$x^{12} \equiv 16, \qquad x^{48} \equiv 9, \qquad x^{20} \equiv 13, \qquad x^{11} \equiv 9.$$

c) In general, if p is a prime and $a \not\equiv 0 \pmod{p}$, how many solutions are there to the equation $x^n \equiv a$? (Hint: either there are no solutions, or there are solutions; the distinction between existence and nonexistence of solutions depends on the index of a. When solutions exist, the number of solutions depends only on p and on n, but not on a.)

Exercise 5.4: (This exercise will require a fair amount of raising numbers to high powers mod 101; be prepared for frequent use of the repeated squaring algorithm from Page 168 of Section 8.2 of Davenport.)

a) Show that 2 is a primitive root mod 101.

b) With respect to the primitive root 2, find the index (i.e., discrete logarithm) of each of 100, 10, -10, 20, -20, and 11 (mod 101). Hints: find the index of $100 \equiv -1$ by using a theorem from class, or from the fact that if you know the index of n^2, you only have two choices for the index of n. From the above fact, you can also get the indices of 10 and of -10. Use these results to easily find the indices of 20 and -20. Lastly, use the fact that $11^2 \equiv 20 \pmod{101}$ to narrow down the search for the index of 11.

c) (Challenge) Find the index of 17 without using a computer or programmable calculator. This should give you some feeling of how annoying it is to find the discrete logarithm. If you are stuck, do some research to find algorithms that are faster than simply listing all the powers of $\overline{2}$ in $\mathbf{Z}/101\mathbf{Z}$.