Math 255 - Spring 2017
Homework 9

This homework is due on Monday, April 10 by 5pm. Please support every assertion that you make with either a precise reference from the textbook (theorem number or page) or provide a proof.

1. (a) Find a primitive root r of 11.
   (b) For this primitive root r, compute $\log_r a$ for each $a \in (\mathbb{Z}/11\mathbb{Z})^\times$.
   (c) Using your computations in part (b), solve the congruences
      i. $7x^3 \equiv 3 \pmod{11}$
      ii. $3x^4 \equiv 5 \pmod{11}$
      iii. $x^8 \equiv 10 \pmod{11}$
2. Let $n = 101$. The goal of this problem will be to compute $\log_3 17$ in $(\mathbb{Z}/101\mathbb{Z})^\times$. We will use a simplified version of the index calculus attack.
   (a) We will first compute $\log_3 2$ in $(\mathbb{Z}/101\mathbb{Z})^\times$. We do this by following these steps:
      - Compute 2^7 and reduce your answer modulo 101.
      - Factor the new number that you obtained.
      - This should give you an equation satisfied by $\log_3 2$. Solve this equation.
   (b) What is $17^{-1} \pmod{101}$? Compute this number and call it b.
   (c) Use that $17b \equiv 1 \pmod{101}$ to get a relationship between $\log_3 2$ and $\log_3 17$. Using the value of $\log_3 2$ you computed in part (a), solve this equation for $\log_3 17$.