

Some notes on the homework assignment:

- Remember to acknowledge your collaborators and cite your sources. The template has a section built in for you to do this (see the comments in the template).
- Remember to let me know if you can't do your peer review this week (for any reason)!

Here's the schedule of when things are due for this assignment.

Component Due	Date
Draft of Solutions	Thursday, May 19
Peer Review	Tuesday, May 24
Final Copy	Friday, May 27

And finally, here are the problem statements.

1. Suppose that  $m$  has a primitive root. Show that the product of all elements of  $(\mathbb{Z}/m\mathbb{Z})^\times$  is congruent to  $-1 \pmod{m}$ .  
*Hint: This reduces to Wilson's Theorem when  $m$  is prime.*
2. Suppose that  $m$  has a primitive root,  $r$ . Show that  $a \equiv b \pmod{m}$  if and only if  $\text{ind}_r(a) \equiv \text{ind}_r(b) \pmod{\varphi(m)}$ .  
*Note: This shows that "taking indices is invertible."*
3. For which positive integers  $a$  is the congruence  $ax^4 \equiv 2 \pmod{13}$  solvable?
4. Let  $N = 2^j u$  be a positive integer where  $j \geq 0$  and  $u$  is odd. Let  $p$  be an odd prime and factor  $p-1 = 2^s t$  where  $s$  and  $t$  are positive integers with  $t$  odd. Show that if  $0 \leq j < s$ , then there are  $2^j(t, u)$  incongruent solutions of  $x^N \equiv -1 \pmod{p}$ . Show that there are no solutions otherwise.