

Math 322 Fall 2017  
Number Theory HW 6  
Due Friday, October 20

You may *not* discuss the starred problem with classmates, though you should of course feel free to discuss it with me as much as you like. Linguistic precision is important for this problem.

(★) **Starred Problem:** Let  $n$  and  $a$  be positive integers. Suppose  $b$  is an inverse of  $a$  modulo  $n$ , and  $n$  is a pseudoprime to the base  $a$ . Show that  $n$  is a pseudoprime to the base  $b$ .

For the remainder of these problems, I encourage you to collaborate with your classmates, as well as to discuss them with me.

1. (a) Compute  $4^{500} \pmod{11}$ .  
(b) Find an inverse for 8 modulo 17.
2. If  $p$  is an odd prime, show that  $2(p-3)! \equiv -1 \pmod{p}$ .
3. 119 is not prime, but we can still use Fermat's little theorem to attempt to compute  $4^{129} \pmod{119}$ .
  - (a) Compute  $4^{129} \pmod{7}$ .
  - (b) Compute  $4^{129} \pmod{17}$ .
  - (c) Use the Chinese Remainder Theorem to compute  $4^{129} \pmod{119}$ .
4. A Fermat number is a number  $F_m = 2^{2^m} + 1$ . Fermat conjectured that every Fermat number is prime; indeed, the first five Fermat numbers (starting with  $m = 0, F_m = 3$ ) are prime. However, so far we have not found  $F_m$  with  $m > 4$  to be prime.  
Prove that if  $F_m$  is composite, it is pseudoprime to the base 2.
5. Show that  $2821 = 7 \cdot 13 \cdot 31$  is a Carmichael number.
6. Show that 25 is a strong pseudoprime to the base 7.