Math 322 Fall 2017
Number Theory HW 6 Solutions
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.

($\star$) **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 $4^{500} \mod 11$.

   Solution:
   $$4^{500} = (4^{10})^{50} \equiv 1^{50} \equiv 1 \mod 11.$$

   (b) Find an inverse for 8 modulo 17.

   Solution: By Fermat's Little Theorem, we know that 8^{15} is an inverse of 8 modulo 17. So we compute
   $$8^{15} = 2^{45} = (2^4)^{11} \cdot 2 = 16^{11} \cdot 2 \equiv (-1)^{11} \cdot 2 \equiv -2 \equiv 15 \mod 17.$$

2. If p is an odd prime, show that $2(p-3)! \equiv -1 \mod p$.

   Solution: Since p is an odd prime, $p \geq 3$ so $(p-3) \geq 0$.

   By Wilson's theorem, we know that $(p-1)! \equiv -1 \mod p$. But
   $$(p-1)! = (p-1)(p-2)(p-3)! \equiv (-1)(-2)(p-3)! \equiv 2(p-3)! \mod p$$

   Thus $2(p-3)! \equiv -1 \mod p$.

3. 119 is not prime, but we can still use Fermat's little theorem to attempt to compute $4^{129} \mod 119$.

   (a) Compute $4^{129} \mod 7$.

   Solution:
   $$4^{129} = (4^6)^{21} \cdot 4^3 \equiv 4^3 \equiv 1 \mod 7.$$

(b) Compute $4^{129} \mod 17$.

Solution:

$$4^{129} = (4^{16})^8 \cdot 4 \equiv 4 \mod 17$$

(c) Use the Chinese Remainder Theorem to compute $4^{129} \mod 119$.

Solution: By the Chinese Remainder Theorem, we have

$$4^{129} \equiv 1 \cdot 17 \cdot 5 + 4 \cdot 7 \cdot 5 = 225 \equiv 106 \mod 119.$$

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.

   Solution: We see that $2^{2^m} \equiv -1 \mod F_m$. If we raise both sides to the $2^{2^m - m}$ power, we get

$$\begin{aligned} (2^{2^m})^{2^{2^m - m}} &\equiv (-1)^{2^{2^m - m}} \mod F_m \\ 2^{2^m \cdot 2^{2^m - m}} &\equiv 1 \mod F_m \\ 2^{2^{2^m}} &\equiv 1 \mod F_m \\ 2^{F_m - 1} &\equiv 1 \mod F_m. \end{aligned}$$

5. Show that $2821 = 7 \cdot 13 \cdot 31$ is a Carmichael number.

   Solution: Option 1: We observe that $2820 = 6 \cdot 470 = 12 \cdot 235 = 30 \cdot 94$. Thus by our theorem, 2821 is a Carmichael number.

   Option 2: Suppose $(b, 2821) = 1$. Then in particular, $(b, 7) = (b, 13) = (b, 31) = 1$. We compute

$$\begin{aligned} b^{2920} = (b^6)^{470} &\equiv 1 \mod 7 \\ b^{2920} = (b^{12})^{235} &\equiv 1 \mod 13 \\ b^{2920} = (b^{30})^{94} &\equiv 1 \mod 31 \end{aligned}$$

   and then by the Chinese Remainder Theorem, $b^{2820} \equiv 1 \mod 7 \cdot 13 \cdot 31$. Thus by definition 2821 is pseudoprime to the base b for any b with $(b, 2821) = 1$, and thus by definition 2821 is a Carmichael number.

6. Show that 25 is a strong pseudoprime to the base 7.

   Solution: Note that $7^2 = 49 \equiv -1 \mod 25$. Thus $7^{24} \equiv (-1)^{12} \equiv 1 \mod 25$, so 25 is a pseudoprime to the base 7 (since $25 = 5 \cdot 5$ is composite).

   Now we apply Miller's test. $24 = 2^3 \cdot 3$. We compute

$$\begin{aligned} 7^{12} &\equiv (-1)^6 \equiv 1 \mod 25 \\ 7^6 &\equiv (-1)^3 \equiv -1 \mod 25 \end{aligned}$$

   Thus $7^{2 \cdot 3} = 7^{24/4} \equiv -1$ so 25 passes the Miller test for the base 7, and by definition 25 is a strong pseudoprime to the base 7.