Ideas in Mathematics
Math 170, Spring 2016
Assignment 9, part 1

1. For each base a and modulus m determine the pattern $a^1, a^2, a^3, \ldots \pmod{m}$.

- $a = 3$, $m = 4$ $\quad 3, 1, 3, 1 \ldots$
- $a = 7$, $m = 9$
- $a = 4$, $m = 5$
- $a = 5$, $m = 9$
- $a = 4$, $m = 9$
- $a = 5$, $m = 11$
- $a = 5$, $m = 8$
- $a = 5$, $m = 13$

2. Use Fermat's Little Theorem to solve the following congruence relations. Each should be solved with a number in $\{0, 1, \ldots, m-1\}$, where m is the modulus; in all cases here, the modulus m is a prime number.

- $194^{12} \equiv 1 \pmod{13}$
- $2^{12603} \equiv \quad \pmod{127}$
- $250^{16} \equiv \quad \pmod{17}$
- $3^{1360} \equiv \quad \pmod{137}$
- $591^{100} \equiv \quad \pmod{11}$
- $19^{12006} \equiv \quad \pmod{13}$
- $194^{60} \equiv \quad \pmod{7}$
- $14^{1201} \equiv \quad \pmod{13}$

3. In class we discussed the difficulty of computing the "logarithm" of a number in modular arithmetic. Determine the smallest $n > 0$ for which each congruence relation is true.

- $3^n \equiv 1 \pmod{5}$ $\quad n = 4$
- $17^n \equiv 95 \pmod{101}$
- $3^n \equiv 2 \pmod{5}$
- $9^n \equiv 5 \pmod{11}$
- $5^n \equiv 2 \pmod{7}$
- $13^n \equiv 1 \pmod{15}$
- $13^n \equiv 7 \pmod{10}$
- $5^n \equiv 3 \pmod{23}$

Ideas in Mathematics
Math 170, Spring 2016
Assignment 9, part 2

4. In the Diffie-Hellman key-exchange protocol, a base g and a modulus m are agreed upon publicly. Alice then chooses a secret number a and Bob chooses a secret number b. Alice can then tell Bob, and the whole world if she wants, the number $g^a \pmod m$ and Bob can tell everyone the number $g^b \pmod m$. Bob, who knows b, computes $(g^a)^b \pmod m$, and Alice, who knows a, computes $(g^b)^a \pmod m$. Notice that $(g^a)^b = (g^b)^a$, and so Alice and Bob now share a secret number that no other person knows.

   Let $g = 3$ and $m = 127$, and assume that Alice has chosen 11 and Bob has chosen 14. First, compute the numbers g^a and $g^b \pmod m$. Next compute $(g^a)^b$ and $(g^b)^a \pmod m$. Are the numbers the same?

5. CORRECTED: In the problem above, we chose the number g so that the sequence $g^1, g^2, g^3, \ldots \pmod m$ is very long (its period is 126). However, had we chosen another number, our period could be much shorter. For example, if $g = 4$, then the period of the pattern is only 7 (the following sequence repeats: 4, 16, 64, 2, 8, 32, 1). Why is it important that we choose a g so that the pattern is very long? What would happen if the pattern is very short? This question requires thinking.

6. How would you figure out the last two digits of 31^{1000}? What are those last two digits? As a hint, think about what the last digit of 31^{1000} must be.