HW 8, Due Jan 14

READ THE NOTES ON FINDING PRIMES.

1. (20 points) Find THREE solutions to

   $$x^2 + 9x + 20 \equiv 0 \pmod{1892}$$

   (NOTE- the solutions are in $\{0, 1, 2, \ldots, 1891\}$.) DO NOT use Brute Force. Use the method I showed in class.

2. (20 points) (For this problem you can use the Web, but please cite your sources.) Find THREE numbers $n \ge 100$ such that n is composite BUT for all $a \in \{0, 1, 2, \ldots, n-1\}$, $a^{n-1} \equiv 1 \pmod{n}$. (This shows that the primality test I gave in class can FAIL on a number.)

3. (20 points) For all $a \in \{1, \ldots, 20\}$ compute $a^{20} \pmod{21}$. How many of them are 1? (We are hoping that not that many are 1 so that in this case the primality test will discover that 21 is NOT a prime QUICKLY.)

4. (20 points) Write CODE for the primality-test I gave in class that will STOP as soon as you find the number is NOT prime. (Note that this will be FASTER than my code.) Your psudeocode can use expressions like *If a^{n^2} is a zell composite then* .

5. (20 points) Bob wants to write program that will, given n, find a prime p between n and $2n$. Bob knows that $p \not\equiv 0 \pmod{2}$, $p \not\equiv 0 \pmod{5}$, and $p \not\equiv 0 \pmod{7}$ but somehow Bob DOES NOT KNOW that $p \not\equiv 0 \pmod{3}$. This problem will guide you through Bob's thought process and result in the program that Bob wants. Note that $2 \times 5 \times 7 = 70$.

   (a) Find a set $A \subseteq \{0, \ldots, 69\}$ such that
   $(n \not\equiv 0 \pmod{2}$ AND $n \not\equiv 0 \pmod{5}$ AND $n \not\equiv 0 \pmod{7})$
   IFF
   $(\exists a \in A)[n \equiv a \pmod{70}]$.

   (b) Use this set A to write code that will, given n, find a prime between n and $2n$.

   (c) Modify your code to find a SAFE PRIME between n and $2n$.