HOMEWORK ASSIGNMENT #5, DUE FRIDAY, 10/29/2010

This assignment has certain problems which require a fair amount of numerical calculation. Each problem has slightly different guidelines for the amount of calculation you should show on your work, so please check them carefully.

(1) Using the fast exponentiation algorithm for numbers mod n, compute $5^{87} \mod 307$ (that is, find the remainder when you divide 5^{87} by 307.) You can use a calculator to square numbers mod 307, and multiply individual numbers mod 307, but you should do the calculation of the binary expansion of the exponent by hand, list the appropriate table of powers of 5, and indicate why you are multiplying the correct powers together.

(2) Show that 671 is a Fermat psuedoprime to the base 3. Same computational rules as the previous question.

(3) Show that $1105 = 5 \cdot 13 \cdot 17$ is a Carmichael number. Your should only use a calculator to check whether a number is a divisor of another number.

(4) Show that 2047 is a strong psuedoprime to the base 2. For this problem you should not use a calculator, at all. (There is probably a clever way to solve this problem. How are 2047 and 2 related?)

(5) Show that 91 is a psuedoprime to base 3, but not a strong psuedoprime to base 3. Same computational rules as the first two questions.

(6) Let $a \geq 2$ be a positive integer, and let p be an odd prime not dividing $a^2 - 1$. Show that $\dfrac{a^{2p}-1}{a^2-1}$ is a Fermat psuedoprime to the base a. (Notice, in particular, that this implies that there are infinitely many Fermat psuedoprimes to base a.)

(7) Find all solutions to $x^2 + 3x + 7 \equiv 0 \mod 5^3$. You should not use a calculator for this problem.

(8) (a) Show that $x^2 \equiv 2 \mod 5^n$ has no solution, for any $n \geq 1$.
(b) Show that $x^2 \equiv 2 \mod 7^n$ has a solution, for any $n \geq 1$.