M445/845, Homework 3, due Monday, October 14, 2013

Instructions: Do any three problems.

(1) Let $n > 1$ be an integer. Prove that $(n-1)! \equiv -1 \mod n$ if and only if n is prime.

(2) Let p be a prime and let b, $1 \leq b < p$, be an integer. We say that b is a *quadratic residue* modulo p if $x^2 \equiv b \mod p$ has a solution. If p is an odd prime, show that there are exactly $(p-1)/2$ quadratic residues $1 \leq b < p$.

(3) Let p be a prime. Fermat's Little Theorem states that $a^{p-1} \equiv 1 \mod p$ whenever a is an integer with $(a, p) = 1$. For the rest of this problem, assume p is an odd prime.
   (a) Use Fermat's Little Theorem to show that $a^{(p-1)/2} \equiv \pm 1 \mod p$ whenever a is an integer with $(a, p) = 1$.
   (b) Let a be an integer. If $a^{(p-1)/2} \equiv -1 \mod p$, show that $x^2 \equiv a \mod p$ has no solution.

(4) A fact known as Euler's criterion is that if p is an odd prime and a is an integer with $(a, p) = 1$, then $x^2 \equiv a \mod p$ has a solution if and only if $a^{(p-1)/2} \equiv 1 \mod p$. Problem 3(a, b) shows the only if implication. Prove the if implication in case $p \equiv 3 \mod 4$. I.e., when $p \equiv 3 \mod 4$, show that $x^2 \equiv a \mod p$ has a solution if $a^{(p-1)/2} \equiv 1 \mod p$. [Hint: show that $x = a^{(p+1)/4}$ is a solution in this case.]

(5) Solve the following quadratic congruence equations, or show that no solutions exist. (You could of course write a computer program program and do this by brute force, but the idea here is to use techniques from previous problems, together with completing the square. You may assume Euler's criterion, and feel free to use the class computational website to compute modular powers.)
   (a) $x^2 + 3x + 3 \equiv 0 \mod 17$
   (b) $x^2 + 3x + 3 \equiv 0 \mod 19$

(6) The Boeing 787 Dreamliner is a long-range, mid-size, wide-body, carbon fiber composite, twin-engine, fly-by-wire jet airliner developed by Boeing Commercial Airplanes, seating from 210 to 330 passengers. It's one of the most advanced passenger airliners in the air today. Also, as it happens, 787 is prime. Using the methods developed above (and the class computation website, if you like, to do modular powers), solve the equation $x^2 + 247x + 44 \equiv 0 \mod 787$, or show that no solution exists.