Math 567, Assignment #4

(due February 24)

1. Fix $n > 1$ and $1 \leq k \leq n-1$. Show that k has a multiplicative inverse modulo n if and only if $\gcd(k, n) = 1$.

2. One of the puzzles Fermat posed was that of showing that the only solutions of $y^2 = x^3 - 4$ in whole numbers are $(2, 2)$ and $(5, 11)$. Fermat's English antagonist John Wallis derided such puzzles and posed some of his own, intending them as counter-challenges — such as the problem of finding all whole-number solutions to $y^2 = x^2 - 15$. But Wallis missed the point entirely and failed to see how different these two puzzles are. Use the identity $x^2 - y^2 = (x + y)(x - y)$ as an aid in solving Wallis' puzzle.

3. (a) Find the units digit of 3^{100} by using Fermat's Theorem.
(b) Verify that for any positive integer a, a^5 and a have the same units digit.

4. (a) Let p be a prime and $\gcd(a, p) = 1$. Use Fermat's Theorem to verify that $x \equiv a^{p-2}b \pmod{p}$ is a solution of the linear congurence $ax \equiv b \pmod{p}$.
(b) By applying part (a), solve the (individual) congruences $2x \equiv 1 \pmod{31}$, $6x \equiv 5 \pmod{11}$, and $3x \equiv 17 \pmod{29}$.

5. Establish the congruence

$$2222^{5555} + 5555^{2222} \equiv 0 \pmod{7}.$$

(*Hint*: First evaluate 1111 modulo 7.)

6. (a) Show that no prime of the form $4k + 3$ can divide a number of the form $n^2 + 1$. (*Hint*: Use Theorem 5.5.)
(b) Show that for any N, $4N^2 + 1$ must be divisible by a prime of the form $4k + 1$ that is not a factor of N.
(c) Use this to show that there are infinitely many primes of the form $4k + 1$.