189-235A: Basic Algebra I
Assignment 3

Due: Wednesday, September 25.

Section 2.1: 11,15, 30. **Section 2.2**: 3, 6, 10. **Section 2.3**: 2,3,4.

10. (Fermat's little theorem and primality testing).
a) Show that p is prime if and only if p divides the binomial coefficient $\binom{p}{k}$ for all $1 \leq k \leq p-1$.
b) Show that if p is prime, then $a^p \equiv a \pmod{p}$ for all integers a. This is known as Fermat's little theorem.
c) Show that if $n = 1729$, then $a^n \equiv a \pmod{n}$ for all a, even though n is not prime. Hence the converse to b) is not true. An integer which is not prime but still satisfies $a^n \equiv a \pmod{n}$ for all a is sometimes called a strong pseudoprime, or a Carmichael number. It was shown only three years ago by A. Granville that there are infinitely many Carmichael numbers. Incidentally, the integer 1729 was the number of Hardy's taxicab, and Ramanujan noted that it is remarkable for other reasons as well. (See *A mathematician's apology* by G.H. Hardy.)
d) Using part b), describe an algorithm that can *sometimes* detect whether a large integer (say, of 100 or 200 digits) is composite. It is important that your algorithm be more practical than, say, trial division which would run for well over a billion years on a very fast computer with a number of this size!
e) Show that if p is prime, and $\gcd(a, p) = 1$, then $a^{(p-1)/2} \equiv 1$ or $-1 \pmod{p}$. Show that this statement ceases to be true when $p = 1729$. This remark is the basis for the Miller-Rabin primality test which is widely used in practice.