189-235A: Basic Algebra I
Assignment 3

Due: Wednesday, October 5.

1. Solve the following congruence equations:
(a) $3x \equiv 5 \pmod 7$; (b) $3x \equiv 1 \pmod{11}$;
(c) $3x \equiv 6 \pmod{15}$; (d) $6x \equiv 14 \pmod{21}$.

2. If an integer n is a sum of three perfect squares (i.e., it is of the form $a^2 + b^2 + c^2$ with $a, b, c \in \mathbf{Z}$), show that $n \not\equiv 7 \pmod 8$. Conclude that there are positive integers that cannot be expressed as the sum of three squares. What is the smallest one?

3. Show that $a^5 \equiv a \pmod{30}$, for all integers a.

4. Find an element a of $\mathbf{Z}_{11}$ such that every non-zero element of $\mathbf{Z}_{11}$ is a power of a. (An element with this property is called a *primitive root* mod 11.) Can you do the same in $\mathbf{Z}_{24}$?

5. Prove or disprove: if $x^2 = 1$ in $\mathbf{Z}_n$, then $x = 1$ or $x = -1$.

6. Prove or disprove: if $x^2 = 1$ in $\mathbf{Z}_n$, and n is prime, then $x = 1$ or $x = -1$.

7. Let a and n be integers with $n > 1$. Show that $\gcd(a, n) = 1$ if and only if the congruence class $[a]$ of a in $\mathbf{Z}_n$ is invertible.

8. List the invertible elements of $\mathbf{Z}_5$ and $\mathbf{Z}_{12}$.

9. Show that p is prime if and only if p divides the binomial coefficient $\binom{p}{k}$ for all $1 \leq k \leq p-1$.

10. Using the result of question 9, give an alternate proof of Fermat's little theorem: i.e., show that if p is prime, then $a^p \equiv a \pmod{p}$ for all integers a.

11. 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 10 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 pseudo-prime*, or a *Carmichael number*. It was recently shown that there are infinitely many Carmichael numbers (cf. Alford, Granville, and Pomerance. *There are infinitely many Carmichael numbers*. Ann. of Math. (2) 139 (1994), no. 3, 703–722.) The integer 1729 was the number of Hardy's taxicab, and Ramanujan noted that it is remarkable for other reasons as well. (See G.H. Hardy, *A mathematician's apology*.)

The following problems are for extra credit. Whether you do them or not will not make a big difference in your assignment grade. If you attempt them, I hope you will find them challenging and rewarding.

12. Using 10, 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!

13. 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.