189-235A: Basic Algebra I
Assignment 2

Due: Monday, October 7.

1. Let R be the set of elements of the form $a + b\sqrt{-5}$, where a and b are in $\mathbf{Z}$. Show that R is a ring by using the fact that you already know this for the complex numbers. An element p of R is said to be a *prime in R* if any divisor of p in R is either 1, -1, p, or $-p$. Show that $p = 3$ is a prime in R. Find elements x and y in R such that $p = 3$ divides xy but p divides neither x nor y. (This shows that the analogue of Gauss's lemma fails to be true in R.)

2. Solve the following congruence equations:
   (a) $4x \equiv 3 \pmod 7$; (b) $5x \equiv 2 \pmod{11}$;
   (c) $3x \equiv 6 \pmod{15}$; (d) $6x \equiv 14 \pmod{21}$.

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

4. Find an element a of $\mathbf{Z}/13\mathbf{Z}$ such that every non-zero element of this ring is a power of a. (An element with this property is called a *primitive root* mod 13.) Can you do the same in $\mathbf{Z}/24\mathbf{Z}$?

5. Prove or disprove: if $a^2 = b^2$ in $\mathbf{Z}/n\mathbf{Z}$, and n is prime, then $a = b$ or $a = -b$. Give an example, when n is not prime, of two elements of $\mathbf{Z}/n\mathbf{Z}$ whose squares are equal, yet are not equal up to sign.

6. List the invertible elements of $\mathbf{Z}/24\mathbf{Z}$ and $\mathbf{Z}/9\mathbf{Z}$.

7. Prove that the integer 437 is composite *without* attempting to factor it, by computing 2^{437} in $\mathbf{Z}/437\mathbf{Z}$. It is OK (in fact, it is advised) to use a calculator, but clearly indicate the steps in your calculation. (You need not be fastidious in justifying your arithmetic in $\mathbf{Z}/437\mathbf{Z}$, though. So it is perfectly OK to write $512 = 75$ or $436 = -1$ without further ado.)

8. 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 Fermat's Little Theorem 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 is known 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.*)

9. Show that if p is prime, and $\gcd(a, p) = 1$, then $a^{(p-1)/2} \equiv 1$ or $-1 \pmod{p}$. More generally, show that if $p - 1 = 2^r m$ with m odd, the sequence

$$(a^{(p-1)}, a^{(p-1)/2}, a^{(p-1)/4}, \ldots, a^{(p-1)/2^r})$$

(taken modulo p) starts of with sequence of 1's, and that the first term that differs from 1 is equal to $-1 \pmod{p}$. 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.

10. A mathematician with relationship problems remarks to another "I only love those who do not love me. In fact, the people I love are *precisely* those who do not love me." He is told "In that case, you do not exist." Explain the punch line. (This is a good example of a joke that only mathematicians find amusing. You may want to reflect on the relation with the somewhat subtle question 11 of the previous assignment.)