189-235A: Basic Algebra I
Assignment 2

Due: Wednesday, October 10.

1. Let R be the set of elements of the form $a + b\sqrt{-11}$, where a and b are in $\mathbf{Z}$. 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. An integer is said to be N-smooth if all its prime divisors are less than or equal to N. Show that

$$\prod_{p \leq N} \frac{1}{1 - \frac{1}{p}} = \sum_{n \ N-smooth} \frac{1}{n},$$

where the product on the left is taken over the primes less than N, and the (infinite) sum on the right is taken over all the N-smooth integers $n \geq 1$. (Hint: remember how to sum an infinite geometric series! Note also the crucial role played by the fundamental theorem of arithmetic in your argument.)

3. Show that

$$\lim_{N \longrightarrow \infty} \left(\prod_{p \leq N} \frac{1}{1 - \frac{1}{p}} \right) = \infty,$$

and conclude that there are infinitely many primes. This remarkable proof was discovered by Leonhard Euler.

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

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

6. Find an element a of $\mathbf{Z}/11\mathbf{Z}$ 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 11.) Can you do the same in $\mathbf{Z}/24\mathbf{Z}$?

7. Prove or disprove: if $x^2 = 1$ in $\mathbf{Z}/n\mathbf{Z}$, and n is prime, then $x = 1$ or $x = -1$. What if n is not prime?

8. List the invertible elements of $\mathbf{Z}/5\mathbf{Z}$ and $\mathbf{Z}/12\mathbf{Z}$.

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, prove that if p is prime, then $a^p \equiv a \pmod{p}$ for all integers a (Fermat's little theorem) by induction on 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 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*.)

12. Using Fermat's little theorem, 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 $-1 \pmod{p}$. 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.