Suggested reading: Trappe-Washington Ch 3.1 – 3.3. **Note:** this assignment does *not* need to be typed.

This assignment includes four optional "challenge" problems. These are not for credit, though you may do a challenge problem in the place of one of the first ten problems (or two challenge problems instead of two standard problems, etc) for credit. This offer is intended so more advanced students do not need to re-do questions they have done before or would find redundant. You are responsible for understanding the solutions to the standard problems, so I suggest against a swap unless you are confident you could solve the standard problem. Of course, anyone is welcome to do more than ten problems.

1. (a) Define the phrase m *divides* n.
   (b) Given integers m and n, state the definition of the *greatest common divisor* of m and n.
   (c) Suppose that m and n are two integers such that $m \mid n$. Find $\gcd(m, n)$, and prove your solution.

2. (a) Find the greatest common divisor of 1064 and 856.
   (b) Find integers x and y so that $1064x + 856y = \gcd(1064, 856)$.

3. Complete our proof that the Euclidean algorithm computes the gcd, by showing for $a, b, q, r \in \mathbb{Z}$ with $a = bq + r$ then $\gcd(a, b) = \gcd(b, r)$.
   Hint: Show that any common divisor of a and b is also a common divisor of b and r, and vice versa. If the set of common divisors of a and b is the same as the set of common divisors of b and r, then both must have the same greatest common divisor.

4. Prove that if $a \in \mathbb{Z}$ such that $a > 1$, then a factors as a product of positive primes, and this factorization is unique up to the order of the factors.
   Hint: This result is proven on page 65 of the textbook. You're welcome to read this proof, but be sure to write up your solution in your own words. Remember that we have already proved in class the following result: If p is prime and p divides a product of integers ab, then $p \mid a$ or $p \mid b$.

5. In this problem, we will give a classical proof of the infinitude of primes.
   (a) Prove that for any $n \in \mathbb{Z}$, $\gcd(n, n + 1) = 1$. Conclude that if a prime p divides n, then p cannot divide $n + 1$.
   (b) Write a proof that there are infinitely many prime numbers, as follows. Assume that there were only finitely many primes $p_1, p_2, \ldots, p_N$. Consider the number $(p_1 p_2 \cdots p_N + 1)$, and use Part (a) to reach a contradiction.

6. Given integers a, b, for what integers d does the equation $ax + by = d$ have integer solutions (x, y)? Justify your answer.

7. (a) We saw in class that $\gcd(28, 80) = 4$, and that the equation $80u + 28v = 4$ has solution $u = -1$ and $v = 3$. There are, however, other solutions (u, v). Describe the set of all integer solutions to $80u + 28v = 4$. *Hint:* If we increase or decrease $u = -1$ by adding a multiple of $\frac{28}{4} = 7$, what can we do to $v = 3$ to compensate?
   (b) We proved that if $a, b \in \mathbb{Z}$ and $\gcd(a, b) = d$, then there exists a solution $u, v \in \mathbb{Z}$ to $au + bv = d$. Assuming $u = u_o$ and $v = v_o$ is one solution, describe the set of all integer solutions (u, v).

8. (a) Let $a, n \in \mathbb{Z}$, $n > 0$. Define the *congruence class of a modulo* n, and describe the set $\mathbb{Z}/n\mathbb{Z}$.
   (b) Explain in your own words what it means to say that "addition and multiplication of congruence classes modulo n are well-defined".
   (c) If $a \equiv b \pmod{n}$ and $k \mid n$, must $a \equiv b \pmod{k}$? Justify your answer.

9. Prove that a has a multiplicative inverse (mod n) if and only if $\gcd(a, n) = 1$.

10. Find a multiplicative inverse for 27 (mod 80).

11. **(Optional – Challenge Question)** Prove that if p is prime, then for any $a, b, n \in \mathbb{Z}$ with $n > 0$,

$$(a+b)^{p^n} \equiv a^{p^n} + b^{p^n} \pmod{p}.$$

This result is affectionately known as "The Freshman's Dream".

12. **(Optional – Challenge Question)** Let $p(x)$ be a polynomial with integer coefficients. A real number z is a *root* of p if $p(z) = 0$. A congruence class $[a]$ modulo n is a *root* of p if $p(a) \equiv 0 \pmod{n}$. A polynomial $p(x)$ of degree d has at most d distinct real roots.

(a) Find a composite number n and a degree d polynomial $p(x)$ with integer coefficients such that more than d distinct congruence classes modulo n are roots of $p(x)$.

(b) Prove that if $q \in \mathbb{Z}$ is prime, and $p(x)$ is a degree d polynomial with integer coefficients, then at most d congruence classes modulo q are roots of $p(x)$. (This question is tricky!)

13. **(Optional – Challenge Question)** Let $\mathbb{Q}[x]$ denote the set of polynomials $f(x)$ with rational coefficients. The goal of this question is to adapt our theory of divisibility to polynomials. Note that a polynomial is called *monic* if its leading coefficient is 1.

(a) What should it mean for a polynomial $f(x)$ to *divide* a polynomial $g(x)$? Define the greatest common denominator of $f(x)$ and $g(x)$. (This should be a monic polynomial that is "greatest" in the sense of having highest degree). What is the analogue of a prime number?

(b) Prove that if $f(x)$, $g(x)$ are nonzero polynomials in $\mathbb{Q}[x]$, then there are polynomials $u(x)$ and $v(x)$ such that $f(x)u(x) + g(x)v(x) = \gcd(f(x), g(x))$. You can adapt our proof from class of the analogous statement for integers, replacing integer inequalities with inequalities involving the polynomials' degrees.

14. **(Optional – Challenge Question)** The Euclidean algorithm also adapts to computing the gcd of polynomials in $\mathbb{Q}[x]$.

(a) Use the Euclidean algorithm and polynomial division to find the gcd $d(x)$ of $(x^5 - x^3 - x^2 + 1)$ and $(x^3 - 2x^2 - x + 2)$.

(b) Find polynomials $u(x)$ and $v(x)$ so that

$$(x^5 - x^3 - x^2 + 1)u(x) + (x^3 - 2x^2 - x + 2)v(x) = d(x).$$