1. Reading
You should read Part 7 in my online notes as well as Chapter 2 of Gilbert/Vanstone.

2. Problems from Gilbert/Vanstone
Exercise Set 2: 11, 18, 27, 30, 36
Problem Set 2: 73

3. Problems from Farshid’s Brain
1. Suppose $a, b, c \in \mathbb{Z}$.
   (a) Show that if $a|b$ and $c \neq 0$, then $ca|cb$.
   (b) Show that if $a|b$ and $b|c$, then $a|c$.
   (c) Show that if $a|b$ and $a|c$, then $a|(mb + nc)$ for all $m, n \in \mathbb{Z}$.

2. Show that there are arbitrarily long sequences of consecutive integers containing no primes. In other words, show that given an integer $N \geq 1$, there exists an integer $a$ such that $a + 1, a + 2, \ldots, a + N$ are all composites. Hint: try $a = N! + 1$. Look for an “obvious” divisor of $a + 1$, an “obvious” divisor of $a + 2$ etc.

3. Suppose $a, b, n$ are integers, $n \geq 1$ and $a = nd + r$, $b = ne + s$ with $0 \leq r, s < n$, so that $r, s$ are the remainders for $a \div n$ and $b \div n$, respectively. Show that $r = s$ if and only if $n|(a - b)$. [In other words, two integers give the same remainder when divided by $n$ if and only if their difference is divisible by $n$.]

4. If $n \geq 1$ and $m_1, \ldots, m_n \in \mathbb{Z}$ are $n$ integers whose product is divisible by $p$, then at least one of these integers is divisible by $p$, i.e. $p|m_1 \cdots m_n$ implies that then there exists $1 \leq j \leq n$ such that $p|m_j$. Hint: use induction on $n$.

5. (a) Calculate gcd(315, 168) using the Euclidean algorithm, then use this information to calculate lcm(315, 168). Determine integers $x, y$ such that $315x + 168y = \gcd(315, 168)$. You may use the Blankinship version of the Bezout algorithm if you wish. Now obtain the prime factorizations of 315 and 168 to double-check your computation of the gcd and lcm of 315 and 168.
   (b) Calculate gcd(89, 148) using the Euclidean algorithm.

6. (a) Show that if $n > 1$ is composite, then there exists $d$ in the range $1 < d \leq \sqrt{n}$ such that $d|n$. (Hint: you might want to use proof by contradiction).
(b) Use (a) to show that if \( n \) is not divisible by any integers in the range \([2, \sqrt{n}]\), then \( n \) is prime.

c) Use (b) to show that if \( n \) is not divisible by any primes in the range \([2, \sqrt{n}]\), then \( n \) is prime.

d) Use the procedure in (c) to verify that 229 is prime.

e) Suppose you write down all the primes from 2 to \( n \). We know that 2 is a prime so we circle it and cross out all other multiples of 2. The next uncrossed number is 3 and we claim that 3 therefore must be prime. Explain why. Now cross out all the multiples of 3. The next uncrossed number is 5 so we claim it must be a prime. We continue in this fashion until we get to \( \sqrt{n} \). Explain why all the remaining numbers are prime. Carry out this procedure for \( n = 100 \) to find all the primes less than 100. This is called the Eratosthenes sieve. (You may want to write them in 10 rows of 10 numbers each).

7. Prove that if \( n \in \mathbb{N} \), then \( \gcd(n, n + 1) = 1 \).

8. Suppose \( x \) is a real number such that \( x + 1/x \) is an integer. Show that \( x^n + 1/x^n \) is also an integer for all \( n \geq 1 \). (Hint: Use complete induction on \( n \)).

9. Here is a “proof” by complete induction that all Fibonacci numbers are even! Your job is to explain the error in the argument.

For \( n \geq 0 \), let \( P(n) \) be the statement that \( F_n \) is even. We will prove \( P(n) \) by complete induction on \( n \). We check the base case, \( P(0) \): \( F_0 = 0 \) is even. Now we move to the induction step: We must show that if \( P(j) \) holds for \( 0 \leq j \leq n \), then \( P(n) \) holds. Well, if \( P(j) \) holds for \( 0 \leq j \leq n \), then \( F_{n+1} = F_{n-1} + F_n \) is even because \( F_{n-1} \) and \( F_n \) are even by \( P(n - 1) \) and \( P(n) \), respectively. By Complete Induction, therefore, \( F_n \) is even for all \( n \geq 0 \).

10. Show that for \( n \geq 2 \), in any set of \( 2^n - 1 \) integers, there is a subset of exactly \( 2^{n-1} \) of them whose sum is divisible by \( 2^{n-1} \). (Hint: use ordinary induction on \( n \); assuming you can do it for any set of size \( 2^k - 1 \), suppose you have a set of size \( 2^{k+1} - 1 \); leaving out one element, get two sets of size \( 2^{k-1} \) which are “nice,” but this is not enough – now use the elements that have not yet been used to get a third nice set of size \( 2^{k-1} \)).

Extra Credit Problems.

A. Let \( a_1, a_2, \ldots, a_{100} \) be a sequence of length 100 in \( \mathbb{N} \). Show that there is a non-trivial subsequence of this sequence whose sum is divisible by 100. In other words, show that there exists an integer \( N \geq 1 \) and integers \( 1 \leq i_1 < i_2 < \cdots < i_N \leq 100 \) such that \( a_{i_1} + a_{i_2} + \cdots + a_{i_N} \) is divisible by 100.

Hint: Use the pigeon-whole principle as applied to the remainders of the numbers when divided by 100.

B. It is a fact, due to Chebyshev, that for any integer \( n \geq 1 \), there exists a prime in the interval \([n, 2n]\). Use this fact to prove that the harmonic numbers defined by

\[
H_k = \sum_{j=1}^{k} \frac{1}{j} = 1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{k},
\]

are not integers for \( k > 1 \).
C. Recalling the Fibonacci numbers from the previous homework, show that

\[ F_n = F_k F_{n-k} + F_{k-1} F_{n-k-1} \quad \text{for } 1 \leq k \leq n - 1. \]

**SuperExtra Credit Problems.**

D. Let \( a_1, a_2, \ldots, a_{51} \) be integers with \( 1 \leq a_i \leq 100 \) for all \( 1 \leq i \leq 51 \). Prove that there exists \( i \neq j \) such that \( a_i | a_j \).

**Super Duper Extra Credit Problems.**

E. Let \( n \geq 1 \) be a positive integer. Suppose you have \( 2n + 1 \) not necessarily distinct positive integers such that whenever one of the numbers is removed, the remaining \( 2n \) numbers can be divided into two groups of size \( n \) that add up to the same number. Show that the numbers are all the same.

To state this more formally, let \( S = \{1, 2, 3, \ldots, 2n, 2n + 1\} \). Suppose \( f : S \to \mathbb{N} \) is a map such that for all \( x \in S \), there exist sets \( T, U \subset S \setminus \{x\} \) such that \( T \cap U = \emptyset \), \( |T| = |U| = n \), and \( \sum_{t \in T} f(t) = \sum_{u \in U} f(u) \). Show that \( f \) is a constant function i.e. for all \( s_1, s_2 \in S \), \( f(s_1) = f(s_2) \).

Hint: It is relatively easy to prove that all the numbers have the same parity. Is this helpful at all?