MODEL ANSWERS TO THE FIRST HOMEWORK

1.1.1 It is straightforward to check the identity
\[ a^s - b^s = (a - b)(a^{s-1} + a^{s-2}b + a^{s-3}b^2 + \cdots + b^{s-1}). \]
If we put \( a = 2^r \) and \( b = 1 \) then we get
\[
M_n = 2^n - 1 \\
= (2^r)^s - 1^s \\
= a^s - b^s \\
= (a - b)(a^{s-1} + a^{s-2}b + a^{s-3}b^2 + \cdots + b^{s-1}) \\
= (2^r - 1)k \\
= kM_r.
\]
Thus \( M_r \) divides \( M_n \).

1.3.1 (i) As \( 0 = 0 \cdot a, \ a = 1 \cdot a \) and \( a = \pm 1 \cdot \pm a \).

It follows that
\[ a|0, \ a|a \] and \( \pm|a \).

(ii) As \( a|b \) we may find \( k \) such that \( b = ka \) and as \( b|c \) we may find \( l \) so that \( c = lb \). Thus
\[
c = lb \\
= l(ka)b \\
= kl(ab).
\]
Thus \( b|c \).

(iii) As \( a|b \) we may find \( k \) such that \( b = ka \) and as \( a|c \) we may find \( l \) so that \( c = la \). Thus
\[
bx + cy = (ka)x + (la)y \\
= (kx + ly)a.
\]
Thus \( a|(bx + cy) \).

1.3.3. (a) It is expedient to extend the Fibonacci sequence by starting at 0 with 0,
\[ 0, 1, 1, 2, 3, \ldots. \]
Let \( P(m, n) \) be the statement that
\[ F_{m+n+1} = F_m F_n + F_{m+1} F_{n+1}. \]
We prove this by induction on $m$ and $n$.
We first check that $P(0, 0)$, $P(1, 0)$, $P(0, 1)$ and $P(1, 1)$ all hold.
When $m = n = 0$ the LHS of the equation is
$$F_{m+n+1} = F_{0+0+1} = F_1 = 1$$
and the RHS of the equation is
$$F_m F_n + F_{m+1} F_{n+1} = F_0 F_0 + F_1 F_1 = 0 + 1 = 1.$$
As both sides are equal, $P(0, 0)$ holds.
When $m = 1$ and $n = 0$, the LHS of the equation is
$$F_{m+n+1} = F_{1+0+1} = F_2 = 1$$
and the RHS of the equation is
$$F_m F_n + F_{m+1} F_{n+1} = F_1 F_0 + F_2 F_1 = 0 + 1 = 1.$$
As both sides are equal, $P(1, 0)$ holds. By symmetry, $P(0, 1)$ also holds.
When $m = 1$ and $n = 1$, the LHS of the equation is
$$F_{m+n+1} = F_{1+1+1} = F_3 = 2,$$
and the RHS of the equation is
$$F_m F_n + F_{m+1} F_{n+1} = F_1 F_1 + F_2 F_2 = 1 + 1 = 2.$$
As both sides are equal, $P(1, 1)$ holds.
Thus $P(0, 0)$, $P(1, 0)$, $P(0, 1)$ and $P(1, 1)$ all hold.
Now assume that $P(i, j)$ holds for all $i \leq p$ and $j \leq q$. Suppose that $p \geq 1$. Let us show that $P(p + 1, q)$ holds. We have
$$F_{p+q+2} = F_{p+q} + F_{p+q+1}$$
$$= F_{p-1} F_q + F_p F_{q+1} + F_p F_q + F_{p+1} F_{q+1}$$
$$= F_{p-1} F_q + F_p F_q + F_p F_{q+1} + F_{p+1} F_{q+1}$$
$$= (F_{p-1} + F_p) F_q + (F_p + F_{p+1}) F_{q+1}$$
$$= F_{p+1} F_q + F_{p+2} F_{q+1},$$
where we used the recursive definition of the Fibonacci numbers for the first line, the inductive hypotheses $P(p-1, q)$ and $P(p, q)$ to get from the first line to the second line, and the recursive definition of the Fibonacci numbers to get from the fourth line to the fifth line.
Therefore $P(p + 1, q)$ holds. We have shown that $P(i, j)$ for all $i \leq p$ and $j \leq q$ implies $P(p+1, q)$. By symmetry, it follows that we can also deduce $P(p, q + 1)$ using the same hypotheses.
This completes the induction and the proof.
(b) Fix \( r \). We prove that \( F_n \) divides \( F_{rn} \) by induction on \( n \). The case \( n = 1 \) is clear as \( F_1 = 1 \) and 1 divides everything. Suppose that the result is true for \( n \). By (a) we have

\[
F_{(r+1)n} = F_{rn}F_{n-1} + F_{(rn-1)}F_n.
\]

As the first term is divisible by \( F_n \) by induction and the second term is visibly divisible by \( F_n \), it follows that \( F_{(r+1)n} \) is divisible by \( F_n \) by 1.3.1. This completes the induction and so \( F_n \) divides \( F_{rn} \) for all \( r \) and \( n \).

1.3.4.

\[
\alpha > \beta = \frac{1 + \sqrt{5}}{2}.
\]

We proceed by induction on \( n \). For \( n = 0 \) we have

\[
F_0 = 0 < 1 = \alpha^n.
\]

For \( n = 1 \), we have

\[
F_1 = 1 < \beta < \alpha = \alpha^n.
\]

Thus the result is true for \( n = 0 \) and \( n = 1 \).

Let \( f(x) = x^2 - x - 1 \). As \( f'(x) = 2x - 1 \), \( f(x) \) is increasing for \( x \geq 1/2 \).

As \( f(\beta) = 0 \) it follows that \( f(\alpha) > 0 \), so that

\[
(1 + \alpha) < \alpha^2.
\]

Now suppose the result is true for all integers up to \( n \), where \( n \geq 2 \). We have

\[
F_{n+1} = F_n + F_{n-1} < \alpha^n + \alpha^{n-1} = \alpha^{n-1}(\alpha + 1) < \alpha^{n-1}(\alpha^2) = \alpha^{n+1}.
\]

This completes the induction and the proof.

1.4.3 (a) By induction on \( n \). Note that the sum ranges over those indices \( m = n - 2k - 1 \) such that \( 1 < m < n \) and \( n - m \) is odd.

If \( n = 1 \) then there are no integers \( 1 < m < 1 = n \). Thus the result is true for \( n = 1 \) for vacuous reasons.

Now suppose the result is true for \( n \).
\[ F_{n+1} = F_n + F_{n-1} \]
\[ > F_n + \sum_{m:1<m<n-1} F_m \]
\[ = \sum_{m:1<m<n+1} F_m. \]

Here all but the last sum run over integers \( m \) such that \( n-1-m \) is odd and the last one runs over integers \( m \) such that \( n+1-m \) is odd. Of course both of these parity conditions are the same. Since \( n+1-n = 1 \) is odd, the last sum includes the index \( m = n \).

(b) We first prove existence. We proceed by induction on \( n \). If \( n = 1 \) then we may take \( m = 1 \) and \( n_m = 2 \); in this case \( 1 = F_2 \).

Suppose the result is true for all integers up to \( n \). Let \( n_1 \) be the largest integer such that \( n+1-F_{n_1} \geq 0 \). Note that \( n_1 \geq 2 \). If \( n+1 = F_{n_1} \) then we are done. Otherwise, by induction we may find an expression of the form
\[ n+1-F_{n_1} = F_{n_2} + F_{n_3} + \cdots + F_{n_m}, \]
where \( m \geq 2 \), \( n_{j-1} > n_j + 1 \), for \( 3 \leq j \leq m \) and \( n_m \geq 2 \).

If \( n_1 = n_2 + 1 \) then
\[ n+1 \geq F_{n_1} + F_{n_1-1} \]
\[ = F_{n_1+1}, \]
which contradicts our choice of \( n_1 \). Thus \( n_1 > n_2 + 1 \). This completes the induction and the proof of existence.

Now we turn to uniqueness. Suppose that we have two expressions of the form
\[ F_{p_1} + F_{p_2} + \cdots + F_{p_m} = F_{q_1} + F_{q_2} + \cdots + F_{q_n}, \]
where \( m \) and \( n \geq 1 \), \( p_m \) and \( q_n \) are integers, \( p_i-1 \geq p_1 + 2 \) and \( q_j-1 \geq q_j + 2 \). If there are two indices \( i \) and \( j \) such that \( p_i = q_j \) then we may cancel \( F_{p_i} \) and \( F_{q_j} \) from both sides. Thus we may that there are no common terms. Possibly switching the sides of the equation, we may assume that \( p_1 > q_1 \). By (a) we have that
\[ F_{p_1} > \sum_{m:1<m<p_1} F_m \]
\[ \geq F_{q_1} + F_{q_2} + \cdots + F_{q_n}, \]
a contradiction. This proves uniqueness.

1.4.4 (a) Consider numbers of the form \( 6k + r \), \( 0 \leq r \leq 5 \). There are six possibilities for \( r \), 0, 1, 2, 3, 4 and 5. If \( r = 0 \), 2 or 4 then \( 6k + r \)
is even. If \( r = 0 \) or \( 3 \) then \( 6k + r \) is divisible by \( 3 \). Thus if \( 6k + r \) is a prime, not equal to either \( 2 \) or \( 3 \), then \( r = 1 \) or \( r = 5 \).

(b) We have

\[
(6k + 1)(6l + 1) = 36kl + 6k + 6l + 1
\]

\[
= 6(6kl + k + 1) + 1.
\]

Thus the set \( \{ 6k + 1 \mid k \in \mathbb{Z}, k \geq 0 \} \) is closed under multiplication.

(c) Note that \( 5 = 6 \cdot 0 + 5 \) is a prime of the form \( 6k + 5 \). Suppose that there are only finitely many natural numbers \( k_1, k_2, \ldots, k_a \) such that \( p_i = 6k_i - 1 = 6(k_i - 1) + 5 \) is a prime number. Let

\[
N = 6 \prod_{i=1}^{a} p_i - 1.
\]

Note that \( N = 6k + 5 \), where

\[
k = \prod_{i=1}^{a} p_i - 1.
\]

Consider the prime factors of \( N \). Primes of the form \( 6k + 1 \) are closed under multiplication, so that \( N \) has at least one prime factor which is not of the form \( 6k+1 \). Neither \( 2 \) nor \( 3 \) is a prime factor, by construction. Similarly none of the primes \( p_1, p_2, \ldots, p_a \) are factors of \( N \). This is a contradiction. Thus there are infinitely many primes of the form \( 6k+5 \).

(d) Take \( b = 4 \). Any odd prime is of the form \( 4k+1 \) or \( 4k+3 \). Numbers of the form \( 4k+1 \) are closed under multiplication. \( 3 = 4 \cdot 0 + 3 \) is a prime of the form \( 4k + 3 \). Arguing as in (c) it follows that there are infinitely many primes of the form \( 4k + 3 \).

1.4.9. Suppose that \( N = ab \) is odd, where \( a \) and \( b \) are natural numbers. Possibly swapping \( a \) and \( b \) we may assume that \( a > b \). As \( n \) is odd, \( a \) and \( b \) are odd so that both \( a + b \) and \( b - a \) are even. We may find natural numbers \( x \) and \( y \) such that \( 2x = a + b \) and \( 2y = a - b \).

In this case \( 2(x + y) = 2a \) and \( 2(x - y) = 2b \), so that \( a = x + y \) and \( b = x - y \). But then

\[
N = ab
\]

\[
= (x + y)(x - y)
\]

\[
= x^2 - y^2.
\]

Now \( N = N \cdot 1 \) so that there is always at least one way to write \( N \) as a difference of two squares. It follows that \( N \) is an odd prime if and only if there is exactly one way to write \( N \) as a difference of two squares.