1. Here is a careful proof of Theorem 1.1(4): $a | b$ and $b | a$ imply $a = \pm b$.

**Proof:** Suppose $a | b$ and $b | a$. Then there are integers $m$ and $n$ such that $am = b$ and $bn = a$. Substituting $am$ for $b$ in the second equation gives $amn = a$. We can rewrite this last equation as

$$a(mn - 1) = 0.$$ 

Thus either $a = 0$ or $mn = 1$. If $a = 0$, then $b = 0m = 0$ and we have $a = b$, as required.

If $a \neq 0$, then $mn = 1$, so that $|m| \cdot |n| = 1$. Now $|m|$ and $|n|$ are both positive integers. We claim that $|n| = 1$. If not, then $|n| > 1$, so $|m| = 1/|n| < 1$. But there are no positive integers less than 1. The contradiction shows that $|n| = 1$, so $n = \pm 1$, and $a = \pm b$, as required.

(Notice the slightly sneaky use of facts about the ordering of the integers, viewed as a subset of the real numbers.)

Now prove Theorem 1.1(5): $a | b$, $a > 0$, $b > 0$ imply $a \leq b$.

**Proof:** Suppose $a | b$, $a > 0$, and $b > 0$. Then $ma = b$ for some integer $m$, and since $a > 0$ and $b > 0$, $m$ must be positive. Since $m$ is a positive integer, we must have

$$m \geq 1.$$ 

Since $a > 0$, we may multiply both sides of this inequality by $a$ to get $am \geq a$, and since $am = b$, we have shown that $b \geq a$.

2. (§1.2, problem 24) Show that there are no integers $x$ and $y$ such that $(x, y) = 3$ and $x + y = 100$.

**Proof:** Suppose we are given integers $x$ and $y$ with $(x, y) = 3$ and $x + y = 100$. Then $3 | x$ and $3 | y$, so by Theorem 1.1(3), $3 | (x + y)$. But then we have $3 | 100$, a contradiction.

3. (§1.2, problem 26) Let $s$ and $g > 0$ be given integers. Prove that there exist integers $x$ and $y$ with $x + y = s$ and $(x, y) = g$ if and only if $g | s$.

**Proof:** Suppose we are given integers $x$ and $y$ with $g = (x, y)$ and $s = x + y$. Since $g | x$ and $g | y$, we have by Theorem 1.1(3) that $g | (x + y)$. That is, $g | s$. 


Conversely, suppose we are given integers $g > 0$ and $s$ with $g|s$. Then $s = gm$ for some integer $m$. Let $x = g(m - 1)$ and $y = g$. Then
\[ x + y = gm - g + g = gm = s. \]
We claim that $(x, y) = g$. First, since $g > 0$, Theorem 1.6 tells us that
\[ (x, y) = (g(m - 1), g) = g(m - 1, 1). \]
Next, we know that $(k, 1) = 1$ for any integer $k$ (since $(k, 1)$ is a positive divisor of 1, it can only be 1), so we have
\[ (m - 1, 1) = 1. \]
Putting these results together, we get
\[ (x, y) = g(m - 1, 1) = g \]
as required.

4. (Based on §1.2, problem 33) Let $a$ and $b$ be integers, not both zero. Show that $(a, b) = (a, b, ax + by)$ for all integers $x$ and $y$.

**Proof:** Let $S$ be the set of common divisors of $a$ and $b$ and $S'$ the set of common divisors of $a, b,$ and $ax + by$. We will show that $S = S'$.

First, we remark that $S$ is not empty (because $1 \in S$), and that $S$ is finite, because either $a$ or $b$ is non-zero, and thus has only a finite number of divisors.

Now suppose $d \in S'$. Then $d|a$ and $d|b$, so $d \in S$. Thus $S' \subseteq S$.

Conversely, if $d \in S$, then $d|a$ and $d|b$, so by Theorem 1.1(3), $d|ax + by$. Thus $d \in S'$, and we have $S \subseteq S'$.

This shows that $S = S'$. Since $S$ is a finite, non-empty subset of the integers, it has a greatest element, namely the GCD of $a$ and $b$.

Since $S' = S$, the greatest element of $S'$ (which is the GCD of $a, b,$ and $ax + by$) is equal to the greatest element of $S$.

**Alternate proof:** Let $g = (a, b)$ and $f = (a, b, ax + by)$.

Since $f|a$ and $f|b$, $f$ is a common divisor of $a$ and $b$, and so $f$ cannot exceed the greatest common divisor of $a$ and $b$. That is, $f \leq g$. 
On the other hand, since \( g|a \) and \( g|b \), we know by Theorem 1.1(3) that \( g|(ax + by) \), so \( g \) is a common divisor of \( a, b \), and \( ax + by \). As such, \( g \) cannot exceed the greatest common divisor of \( a, b \), and \( ax + by \). That is, \( g \leq f \).

It follows that \( f = g \), as required. \( \qed \)

5. (§1.2, problem 44.) Let \( a, b, \) and \( c \) be integers, and assume that \( a \) and \( b \) are not both zero. Let \( g = (a, b) \). Prove that \( a|bc \) if and only if \( \frac{a}{g}|c \).

Proof: Since \( g = (a, b) \), we have \( g|a \) and \( g|b \), so \( \frac{a}{g} \) and \( \frac{b}{g} \) are integers.

Suppose \( a|bc \). Then \( bc = am \) for some integer \( m \). Dividing through by \( g \), we get

\[
\frac{a}{g} = \frac{b}{g} = c
\]

so that \( \frac{a}{g} \bigg| \frac{b}{g} \). Now by Theorem 1.7,

\[
\left( \frac{a}{g}, \frac{b}{g} \right) = 1
\]

so by Theorem 1.10, we get

\[
\frac{a}{g} \bigg| c
\]

as required.

Conversely, suppose \( \frac{a}{g} \bigg| c \). Then \( c = m\frac{a}{g} \) for some integer \( m \), so

\[
cg = ma.
\]

Multiplying through by the integer \( \frac{b}{g} \), we get

\[
am \left( \frac{b}{g} \right) = cg \left( \frac{b}{g} \right) = bc.
\]

Since \( m\frac{b}{g} \) is an integer, we have shown that \( a|bc \). \( \qed \)
6. (§1.2, problem 47.) If \(a\) and \(b > 2\) are positive integers, prove that \(2^a + 1\) is not divisible by \(2^b - 1\).

**Proof:** Case 1: Suppose \(a < b\). First observe that since \(b > 2\), we have \(2^b - 1 \geq 4\) so that

\[
1 < 2^{b-1} - 1
\]

Adding this inequality to the inequality \(2^a \leq 2^{b-1}\) (which follows from the hypothesis \(a \leq b - 1\)), we get

\[
2^a + 1 < 2^{b-1} + 2^{b-1} - 1 = 2^b - 1.
\]

Thus in the case that \(a < b\) and \(b > 2\), we have \(2^a + 1 < 2^b - 1\). Since both are positive integers, \(2^b - 1\) cannot possibly divide \(2^a + 1\) (Theorem 1.1(5)).

Case 2: Suppose \(a \geq b\).

In this case, we claim the following

**Lemma:** If \((2^b - 1)|(2^a + 1)\), then \((2^b - 1)|(2^{a-kb} + 1)\) for all integers \(k\) with \(0 \leq k \leq \frac{a}{b}\).

**Proof:** By induction on \(k\).

The base case, with \(k = 0\), is clear, since if \((2^b - 1)|(2^a + 1)\), it follows that \((2^b - 1)|(2^a + 1)\).

For the inductive step, let \(k\) be an integer with \(0 \leq k \leq \frac{a}{b} - 1\), and suppose that

\[
(2^b - 1)|(2^{a-kb} + 1).
\]

Then since \(k \leq \frac{a}{b} - 1\) and \(b > 0\), we know

\[
kb \leq a - b,
\]

that is, \((k + 1)b \leq a\), so that \(a - (k + 1)b\) is a non-negative integer. Then \(2^{a-(k+1)b}\) is an integer, and so by Theorem 1.1(3), we get

\[
(2^b - 1)|(2^{a-kb} + 1) - 2^{a-(k+1)b}(2^b - 1).
\]

Now \(2^{a-kb} + 1 - 2^{a-(k+1)b}(2^b - 1) = 2^{a-(k+1)b} + 1\), so we have shown that

\[
(2^b - 1)|(2^{a-(k+1)b} + 1),
\]

completing the inductive step, and completing the proof of the Lemma.
To finish the proof of the Theorem, we use the division algorithm to write

\[ a = bq + r \]

where \( 0 \leq q \leq \frac{a}{b} \) and \( 0 \leq r < b \).

If \( (2^b - 1)|(2^a + 1) \), then by the Lemma,

\[ (2^b - 1)|(2^{a-qb} + 1), \]

that is, \( (2^b - 1)|(2^r + 1) \). But \( r < b \), so by Case 1, this cannot occur. Thus \( 2^b - 1 \) does not divide \( 2^a + 1 \) for \( b \geq a \).

**Alternate proof:**

**Case 1:** (as above)

**Case 2:** Suppose \( a \geq b \) and \( b \geq 3 \).

We use strong induction on \( a \) to prove the statement "For all integers \( a \geq 3 \), for all integers \( b \) with \( 3 \leq b \leq a \), \( (2^b - 1)|(2^a + 1) \)."

**Base case:** For \( a = 3 \), we need only show that \( 2^3 - 1 \) does not divide \( 2^3 + 1 \). This is clear, because 7 does not divide 9.

**Inductive step:** Let \( a \geq 3 \), and suppose that for every \( k \) with \( 3 \leq k \leq a \), we know that there is no integer \( b \) with \( 3 \leq b \leq k \) such that \( (2^b - 1)|(2^k + 1) \).

We claim that there is no integer \( b \) with \( 3 \leq b \leq a + 1 \) such that \( (2^b - 1)|(2^{a+1} + 1) \). Suppose not. Then there exists an integer \( b \) with \( 3 \leq b \leq a + 1 \) such that

\[ (2^b - 1)|(2^{a+1} + 1). \]

Then since \( b \leq a + 1 \), we know \( a + 1 - b \geq 0 \), so \( 2^{a+1-b} \) is an integer, and by Theorem 1.1(3), it follows that \( 2^b - 1 \) divides \( 2^{a+1} + 1 - 2^{a+1-b}(2^b - 1) = 2^{a+1-b} + 1. \) That is,

\[ (2^b - 1)|(2^{a+1-b} + 1). \]

If \( a + 1 - b < b \), then we have a contradiction with Case 1, since \( 2^b - 1 \) can’t divide \( 2^r + 1 \) for any \( r < b \).

So we may assume that \( a + 1 - b \geq b \). That is, \( b \leq \frac{a + 1}{2} \). Since \( a \geq 3 \), we have

\[ \frac{a + 1}{2} < a \]
so we know $b \leq a$. Furthermore, since $b \geq 3$, we know that $3 \leq a + 1 - b \leq a$.

Thus by the inductive hypothesis, $2^b - 1$ cannot divide $2^{a+1-b} + 1$, and again we have a contradiction.

By induction, we have established that for every $a \geq 3$ and for every $b$ with $3 \leq b \leq a$, $(2^b - 1) \nmid (2^a + 1)$. All other values of $a$ and $b$ are handled in Case 1.

7. (a) Use the Euclidean algorithm to find $(37401, 5853)$.

   **Solution:** Implementing the Euclidean algorithm on a computer, we get the table

<table>
<thead>
<tr>
<th>$q$</th>
<th>$r$</th>
</tr>
</thead>
<tbody>
<tr>
<td>37401</td>
<td>5853</td>
</tr>
<tr>
<td>6</td>
<td>2283</td>
</tr>
<tr>
<td>2</td>
<td>1287</td>
</tr>
<tr>
<td>1</td>
<td>996</td>
</tr>
<tr>
<td>3</td>
<td>291</td>
</tr>
<tr>
<td>2</td>
<td>123</td>
</tr>
<tr>
<td>2</td>
<td>45</td>
</tr>
<tr>
<td>1</td>
<td>33</td>
</tr>
<tr>
<td>2</td>
<td>12</td>
</tr>
<tr>
<td>1</td>
<td>9</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

   The greatest common divisor is 3.

   (b) Find integers $x$ and $y$ such that $20437x + 8538y = 1$.

   **Solution:** Here is an Excel table showing the Euclidean algorithm computations. The table determines that $(20437, 8538)$ is, in fact, 1.
The penultimate line of the table tells us that $-2741 \times 20437 + 6561 \times 8538 = 1$, a fact we easily verify with a calculator.

(c) Find integers $x$, $y$, and $z$ such that $323x + 901y + 1007z = 1$. Outline an algorithm for producing the greatest common divisor of three numbers as a linear combination of the numbers.

**Solution:** Using the Euclidean algorithm, we find that $(323, 901) = 17$, and that

$$17 = 14 \times 323 - 5 \times 901.$$  

Similarly, we have $(901, 1007) = 53$, and

$$53 = 9 \times 901 - 8 \times 1007.$$  

The numbers 17 and 53 are both prime, so clearly $(17, 53) = 1$, and we find that

$$1 = 25 \times 17 - 8 \times 53.$$  

Substituting our expressions above for 17 and 53, we get

$$1 = 25 \times (14 \times 323 - 5 \times 901) - 8 \times (9 \times 901 - 8 \times 1007)$$

$$= 350 \times 323 - 197 \times 901 + 64 \times 1007.$$  

In general, given integers $a$, $b$, and $c$, we may write $(a, b)$ as a linear combination of $a$ and $b$, and then write $(b, c)$ as a linear combination of $b$ and $c$. Having done this, we note that

$$(a, b, c) = ((a, b), (b, c))$$
so we may write \((a, b, c)\) as a linear combination of \((a, b)\) and \((b, c)\), and thus as a linear combination of \(a\), \(b\), and \(c\).