Problem 1. Let $S \subset \mathbb{N}$ be a nonempty bounded set and let $G$ be the set of upper bounds of $S$. Since $S$ has at least one upper bound, $G$ is non-empty. By the well-ordering principle, $G$ has a least element $g$. We only have to check that $g \in S$. Suppose not; since $g$ is the least element of $G$, $g - 1 \notin G$ and it’s not an upper bound of $S$. That is, there must exist $s \in S$ s.t. $s > g - 1$. But this would imply that $g \geq s > g - 1$ and this is a contradiction. We’ve tacitly assumed that $g > 1$, but the case where $g = 1$ is “trivial”.

For the other implication, consider $S \subset \mathbb{N}$, $S \neq \varnothing$. Let $M$ be the set of lower bounds of $S$. $M$ is not empty since $1 \in M$. We claim that $M$ is bounded. If it’s not, then for each $n \in \mathbb{N}$, there is a corresponding number $m_n \in M$ such that $m_n > n$. But this means that there is a sequence of lower bounds increasing to infinity, and this implies that $S$ is empty. So $M$ has a largest element $m$. We only need to show that $m \in S$ and this is nearly identical to the proof above.

Problem 2. Define the statement $P(n) := \sum_{i=1}^{n} i = \frac{n(n+1)}{2}$.

$P(1)$ is true, and assume $P(n)$. We need to show $P(n+1)$ holds:

$$\sum_{i=1}^{n+1} i = \sum_{i=1}^{n} i + n + 1 = \frac{n(n+1)}{2} + n + 1 = \frac{(n+1)(n+2)}{2}.$$ 

Problem 3. We need to show that for $a, b \in \mathbb{Z}$ there exist $q \in \mathbb{Z}$ and $0 \leq r < |b|$ such that

$$a = qb + r.$$ 

The uniqueness of the pair $(q, r)$ is exactly as shown in the textbook and doesn’t involve well-ordering or induction. I leave this aspect to you.

As the problem notes, it’s enough to show this for $a, b > 0$, for all other cases can be inferred from this one (how?). Since we’re asked to prove this by induction, we must choose a variable to induct on. There are only two choices: $a$ or $b$. Let’s try induction on $a$ first. The case $b = 1$ is trivial since we can always choose $(q, r) = (a, 0)$ and we can omit it in the discussion below. Let

$$P(n) := \text{for all } b > 1, \text{ there exist } q, r \text{ s.t. } b = qn + r.$$ 

$P(1)$ is immediate with $(q, r) = (0, 1)$. Assume $P(n)$ and we need to show $P(n+1)$. For any $b > 1$, we have

$$n = qb + r,$$

$$n + 1 = qb + (r + 1).$$

If $r + 1 < b$, we’re fine since $0 \leq r < b$. If $r + 1 = b$, $n + 1 = (q+1)b$. These together imply $P(n+1)$. 

1
Problem 4.
(a) Find $g = \gcd(455, 1235)$.

\[
\begin{align*}
1235 &= 2 \cdot 455 + 325 \\
455 &= 1 \cdot 325 + 130 \\
325 &= 2 \cdot 130 + 65 \\
130 &= 2 \cdot 65
\end{align*}
\]

and so $g = 65$.

(b) Working backwards (eliminating the remainders $325, 130$) we get

\[
\begin{align*}
65 &= 325 - 2 \cdot 130 \\
   &= 1235 - 2 \cdot 455 - 2(455 - 325) \\
   &= 1235 - 2 \cdot 455 - 2(455 - 1235 + 2 \cdot 455) \\
   &= 3 \cdot 1235 - 8 \cdot 455
\end{align*}
\]

(c) We know (Theorem 1.13, Jones) that all solutions of the Diophantine equation

\[
g = 1235x + 455y
\]

are given by

\[
g = 1235(3 - \frac{455}{65}i) + 455(-8 + \frac{1235}{65}i),
\]

for $i \in \mathbb{Z}$.

(d) We just need to use the formula (see Jones)

\[
\text{lcm}(a, b) \cdot \gcd(a, b) = ab
\]

to compute that \(\text{lcm}(1235, 455) = 8645\)

Problem 5. This one is very easy. However, it was so easy that I spent some time struggling with it. Suppose $d = \gcd(a + b, a - b)$. Then by definition there are numbers $k$ and $j$ such that

\[
k d = a + b \\
j d = a - b
\]

and so we have

\[
(k + j)d = 2a \\
(k - j)d = 2b
\]

So clearly, if $d \geq 3$ then $d$ must divide both $a$ and $b$, producing a contradiction.

Problem 6.
(a) Suppose

\[
g = \gcd(a, b).
\]

We need to show that any number $d$ is a divisor of both $a$ and $b$ iff it divides $g$. Suppose $d | g$, then since $a$ and $b$ are just multiples of $g$, $d$ divides both of them.
For the other direction, write
\[ g = ax + by \]
using the Euclidean algorithm. Then
\[ \frac{a}{d}x + \frac{b}{d}y = \frac{g}{d}. \]
Since \( d \mid a \) and \( d \mid b \), the left side is an integer, and hence so is the right side.

(b) If \( m \) is a multiple of the lcm then it certainly is a common multiple of \( a \) and \( b \).

For the other direction, if we know that \( m \) is a common multiple of \( a \) and \( b \), consider

\[ \frac{m}{\text{lcm}(a, b)} = \frac{m}{ab} = \frac{m}{b} \frac{a}{a}x + \frac{m}{a}y. \]

The last expression on the right is an integer, and so it follows that \( m/\text{lcm}(a, b) \) is an integer too, and we’re done.

**Problem 7.** We begin with a lemma that solves item (a)

**Lemma 1.**
\[ \gcd(a_1, a_2, \ldots, a_n) = \gcd(\gcd(a_1, a_2), a_3, \ldots, a_n) \]

**Proof.** Let \( g_1 = \gcd(a_1, a_2, \ldots, a_n) \) and \( g_2 = \gcd(\gcd(a_1, a_2), a_3, \ldots, a_n) \). Since \( g_1 \mid a_1 \) and \( g_1 \mid a_2 \), we have by the previous problem that \( g_1 \mid \gcd(a_1, a_2) \). But we also know that \( g_1 \) divides \( a_3, \ldots, a_n \). So by definition, \( g_1 \) must be smaller than the greatest common divisor of \( \gcd(a_1, a_2), a_3, \ldots, a_n \); i.e.,
\[ g_1 \leq g_2 \]

Similarly, if \( g_2 \) divides each each of \( \gcd(a_1, a_2), a_3, \ldots, a_n \), we must have that \( g_2 \) is a common divisor of \( \{a_1, a_2, \ldots, a_n\} \). This gives,
\[ g_2 \leq g_1. \]

This is a common proof technique. To show two things are equal, first show one is less than the other, and then vice-versa. \( \square \)

The next lemma solves item (b)

**Lemma 2.** For given \( a_1, \ldots, a_n \in \mathbb{Z} \), let \( g = \gcd(a_1, a_2, \ldots, a_n) \). Then, there exist \( x_1, \ldots, x_n \in \mathbb{Z} \) such that
\[ g = \sum_{i=1}^{n} a_i x_i \]

**Proof.** This is by induction. For \( n = 2 \), this is just Bezout’s theorem (see Jones). Assume the result for general \( n \). For \( n + 1 \), let
\[ g_{n+1} = \gcd(a_1, a_2, \ldots, a_n) = \gcd(\gcd(a_1, a_2), a_3, \ldots, a_n) \]
using Lemma 1.

The set \( \{\gcd(a_1, a_2), a_3, \ldots, a_n\} \) has only \( n \) numbers and so we have by the induction assumption
\[ g_{n+1} = x_1 \gcd(a_1, a_2) + \cdots + x_n a_{n+1}. \]
Use Bezout’s theorem to write \( \gcd(a_1, a_2) = pa_1 + qa_2 \) for some numbers \( p, q \) and substitute it into the equation above to get

\[
g_{n+1} = x_1pa_1 + \cdots + x_na_{n+1}.
\]

\( \square \)

Item (c) Suppose there is a solution to

\[
d = \sum_{i=1}^{n} a_ix_i
\]

then \( g = \gcd(a_1, a_2, \ldots, a_n) \) divides the left and right hand sides of the above equation and we get \( g \mid d \). The reverse implication follows from Lemma 2.

Part (d):
We’ll write the general form down for \( n = 3 \). If one number is a multiple of the other, say \( a = kb \), then the equation reduces to the \( n = 2 \) case. We then need to solve

\[
(kx + y)b + cz = d
\]

If this equation has solutions, they are all of the form

\[
(kx + y) = a_0 - ic \frac{c}{\gcd(a,b,c)},
\]

\[
z = z_0 + j \frac{b}{\gcd(a,b,c)}.
\]

To assign values to \( x \) and \( y \), we need to solve \( kx + y = a_0 - ic/\gcd(a,b,c) \). This is again a Diophantine equation in two variables. Further, \( \gcd(k,1) = 1 \), so we know that we always have solutions for \( x, y \) of the form

\[
x = x_0 - j, y = y_0 + jk.
\]

This solves the “degenerate case”.

Now we can assume that no number is a multiple of the other, and this in turn implies that \( \gcd(a,b), \gcd(b,c), \gcd(a,c) \) are not all equal to \( \gcd(a,b,c) \). Define

\[
l_a = \frac{\gcd(b,c)}{\gcd(a,b,c)},
\]

\[
l_b = \frac{\gcd(a,c)}{\gcd(a,b,c)},
\]

\[
l_c = \frac{\gcd(a,b)}{\gcd(a,b,c)}.
\]

We claim that the general solution to (2) is

\[
d = a(x_0 + il_a) + b(y_0 + jl_b) + c(z_0 + kl_c),
\]

where \( ail_a + bjl_b + ckl_c = 0 \). Consider any other solution \( (p,q,r) \) s.t.

\[
d = ap + qb + cr.
\]

Set the two equations above equal to each other to get

\[
0 = a\bar{x} + b\bar{y} + c\bar{z}
\]

where \( \bar{x} = x_0 + il_a - p, \bar{y} = y_0 + jl_b - p \) etc. Divide the equation through by \( \gcd(a,b) \) to get

\[
0 = \frac{a}{\gcd(a,b)} \bar{x} + \frac{b}{\gcd(a,b)} \bar{y} + \frac{c}{\gcd(a,b)} \bar{z}.
\]
The first two terms in the above equation are integers, so the third one must be one too. Rewrite the third term as
\[ \frac{c}{\gcd(a,b,c)} \cdot \frac{\gcd(a,b,c)}{\gcd(a,b)} \cdot \frac{\gcd(a,b,c)}{\gcd(a,b,c)} . \]
Notice that $\gcd(a,b,c) | \gcd(a,b)$ by the previous problem, and $\gcd(a,b,c) | c$. Suppose $\gcd(a,b)/ \gcd(a,b,c)$ divides $c/ \gcd(a,b,c)$. Then
\[ k \cdot \frac{\gcd(a,b)}{\gcd(a,b,c)} = \frac{c}{\gcd(a,b,c)}, \]
which means that $\gcd(a,b)|c$ and hence $\gcd(a,b) = \gcd(a,b,c)$. This would contradict our assumption. So we must have that $\gcd(a,b)/ \gcd(a,b,c)|\bar{z}$ and so
\[ \bar{z} = m \cdot \frac{\gcd(a,b)}{\gcd(a,b,c)}, \]
for some integer $m$. This gives us that $r = z_0 + (i - m) \gcd(a,b)/ \gcd(a,b,c)$. A similar argument can be repeated for $\bar{x}$ and $\bar{y}$.

**Problem 8.** Let $g = \gcd(780, 286, 195) = \gcd(\gcd(780, 286), 195)$. $\gcd(780, 286) = 26$, $\gcd(26, 195) = 13$. We get
\[ 13 = -2 \cdot 286 + 3 \cdot 195, \]
by using the extended Euclidean algorithm twice. Part $c$ is routine: $(0 + 286 \cdot 195, -2 - 780 \cdot 195, 3)$ is another solution.

**Problem 9.** Write $n = q7 + r$ and $r$ can take values from $0, \ldots, 6$. Squaring this, (or working more efficiently in modular arithmetic), get
\[
\begin{align*}
(1 \mod 7)^2 &= 1 \mod 7 \\
(2 \mod 7)^2 &= 4 \mod 7 \\
(3 \mod 7)^2 &= 2 \mod 7 \\
(4 \mod 7)^2 &= 2 \mod 7 \\
(5 \mod 7)^2 &= 4 \mod 7 \\
(6 \mod 7)^2 &= 1 \mod 7 
\end{align*}
\]
to get the possibilities $1, 2, 4$. 