Problem 1:

(a) If \( p > 2 \) is prime then \( p \) is odd and hence not divisible by two. Thus \( p \) can be written as \( p = 2k + 1 \) for some positive integer \( k \). The integer \( k \) is either even or odd. If \( k \) is even then \( k = 2n \) for some \( n \in \mathbb{N} \) and hence \( p = 2k + 1 = 4n + 1 \). If \( k \) is odd then \( k = 2n + 1 \) for some \( n \in \mathbb{N} \) and hence \( p = 2k + 1 = 4n + 3 \).

(b) If \( p > 3 \) then \( p \) is not divisible by two or three. The division algorithm tells us that \( p = 6n + r \) for some \( r \) with \( 0 \leq r < 6 \). If \( r = 0 \) then \( p = 6n \) and hence is divisible by 3, a contradiction. If \( r = 2 \) then \( p = 6n + 2 = 2(3n + 1) \) and hence \( p \) is divisible by 2, another contradiction. Similarly, if \( r = 3 \) then \( 3 \mid p \) and if \( r = 4 \) then \( 2 \mid p \). Therefore, \( p = 6n + r \) where \( r = 1 \) or \( r = 5 \).

(c) As \( p > 2 \) we know from part (a) that either \( p = 4n + 1 \) or \( p = 4n + 3 \) for some \( n \in \mathbb{N} \). Therefore \( p^2 = (4n + 1)^2 = 16n^2 + 8n + 1 \) or \( p^2 = (4n + 3)^2 = 16n^2 + 24n + 9 \). In the first case, \( p^2 = 4(4n^2 + 2n) + 1 \), so \( p^2 = 4m + 1 \) where \( m = 4n^2 + 2n \in \mathbb{N} \). In the second case, \( p^2 = 4(4n^2 + 6n + 2) + 1 \). Therefore \( p^2 = 4m + 1 \) where \( m = 4n^2 + 6n + 2 \in \mathbb{N} \). Therefore, in all cases, \( p^2 \) is of the desired form.

Problem 2:

(a) \( m = 377 \) and \( n = 29 \). Note that 377 = (29)(13). Hence 29 \( \mid \) 377 and \( \gcd(377, 29) = 29 \). Thus \( \gcd(377, 29) = (1) \cdot (29) + (0) \cdot (377) \).

(b) \( m = -231 \) and \( n = 150 \).

\[
\begin{align*}
-231 &= (-2) \cdot 150 + 69 \quad (69 = -231 + (2) \cdot 150) \\
150 &= (2) \cdot 69 + 12 \quad (12 = 150 + (-2) \cdot 69) \\
69 &= (5) \cdot 12 + 9 \quad (9 = 69 + (-5) \cdot 12) \\
12 &= (1) \cdot 9 + 3 \quad (3 = 12 + (-1) \cdot 9).
\end{align*}
\]
Therefore, $\gcd(-231, 150) = \gcd(9, 3) = 3$. Furthermore

\[
3 = 12 + (-1) \cdot 9 = 12 + (-1) \cdot [69 + (-5) \cdot 12]
= (6) \cdot 12 + (-1) \cdot 69 = (6) \cdot [150 + (-2) \cdot 69] + (-1) \cdot 69
= (6) \cdot 150 + (-13) \cdot 69 = (6) \cdot 150 + (-13) \cdot [-231 + (2) \cdot 150]
= (20) \cdot 150 + (-13) \cdot (-231).
\]

Therefore, $3 = \gcd(-231, 150) = (-13) \cdot (-231) + (-20) \cdot 150$.

**Problem 3:**

Since $m$ and $n$ are odd, we can write $m = 2a + 1$ and $n = 2b + 1$, for some integers $a$ and $b$. Now,

\[
m^2 - n^2 = (2a + 1)^2 - (2b + 1)^2 = 4a^2 + 4a - 4b^2 - 4b = 4[a(a + 1) - b(b + 1)].
\]

However, $a(a + 1)$ and $b(b + 1)$ are both even. Thus $a(a + 1) - b(b + 1)$ is even; so we can write $a(a + 1) - b(b + 1) = 2k$ for some integer $k$. Therefore, $m^2 - n^2 = 8k$ and $8 \mid (m^2 - n^2)$. □

**Problem 4:**

Let $d > 0$ be an integer.

(a) First note that since 7 is prime, then showing that $d = 1$ or $d = 7$ is equivalent to showing that $d \mid 7$.

Now, since $d \mid (11k+4)$ and $d \mid (10k+3)$, then $d$ divides any (integral) linear combination of $(11k+4)$ and $(10k+3)$: $d \mid [x((11k+4) + y(10k+3))$ for all integers $x$ and $y$.

In particular, letting $x = 10$ and $y = -11$ yields that $d$ divides $[(10)(11k + 4) + (-11)(10k + 3)] = 40 - 33 = 7$. Therefore $d \mid 7 \iff d = 1$ or $d = 7$. □

(b) Similarly, since 11 is prime, then showing that $d = 1$ or $d = 11$ is equivalent to showing that $d \mid 11$.

Now, since $d \mid (35k+26)$ and $d \mid (7k+3)$, then $d$ divides any (integral) linear combination of $(35k+26)$ and $(7k+3)$: $d \mid [x(35k+26) + y(7k+3)]$ for all integers $x$ and $y$.

In particular, if we choose $x = 1$ and $y = -5$ we obtain that $d$ divides $[(1)(35k + 26) + (-5)(7k + 3)] = 26 - 15 = 11$. Therefore $d \mid 11 \iff d = 1$ or $d = 11$. □
Problem 5:

(a) Since \( d = \gcd(m, n) \), we have that \( d \mid m \) and \( d \mid n \). Thus there exist integers \( q \) and \( q' \) such that \( m = qd \) and \( n = q'd \). Hence \( \frac{m}{d} = q \) and \( \frac{n}{d} = q' \) are integers.

Now, since \( d = \gcd(m, n) \), there exist integers \( x \) and \( y \) such that \( d = xm + yn \). Substituting for \( m \) and \( n \), we get that \( d = xqd + yq'd \) or \( 0 = (xq + yq' - 1)(d) \). The fact that \( d > 0 \) implies that \( 0 = xq + yq' - 1 \). Thus \( 1 = xq + yq' \) or \( 1 = x \frac{m}{d} + y \frac{n}{d} \). Therefore \( \frac{m}{d} \) and \( \frac{n}{d} \) are relatively prime and \( \gcd\left(\frac{m}{d}, \frac{n}{d}\right) = 1 \). \( \square \)

(b) Assume that \( k \mid d \) where \( k > 0 \). Then there exists an integer \( s \) such that \( d = sk \). Furthermore, since both \( d \) and \( k \) are positive, we should have that the integer \( s = \frac{d}{k} \) is positive.

As remarked in part (a), we have that there exist integers \( q \) and \( q' \) such that \( m = qd \) and \( n = q'd \). Thus we have that
\[
m = qsk
\]
and
\[
n = q'sk.
\]
Thus \( \frac{m}{k} = qs \) and \( \frac{n}{k} = q's \) are integers and we have that \( s \mid \frac{m}{k} \) and \( s \mid \frac{n}{k} \). This implies that \( s \mid \gcd\left(\frac{m}{k}, \frac{n}{k}\right) \) by definition of \( \gcd \).

Furthermore, we known that there exist integers \( x \) and \( y \) such that \( d = xm + yn \). Thus \( sk = xm + yn \), or
\[
s = x \frac{m}{k} + y \frac{n}{k}.
\]
Now since \( \gcd\left(\frac{m}{k}, \frac{n}{k}\right) \) divides both \( \frac{m}{k} \) and \( \frac{n}{k} \), it divides any linear combination of \( \frac{m}{k} \) and \( \frac{n}{k} \); in particular it should divide \( x \frac{m}{k} + y \frac{n}{k} = s \). Thus \( \gcd\left(\frac{m}{k}, \frac{n}{k}\right) \mid s \).

We have shown that \( s \mid \gcd\left(\frac{m}{k}, \frac{n}{k}\right) \) and that \( \gcd\left(\frac{m}{k}, \frac{n}{k}\right) \mid s \), where both \( s \) and \( \gcd\left(\frac{m}{k}, \frac{n}{k}\right) \) are positive. This leads us to conclude that
\[
\gcd\left(\frac{m}{k}, \frac{n}{k}\right) = s = \frac{d}{k}.
\]
\( \square \)
Addendum: Solution of #2 and # 5 of the Recommended Practice Problems:

#2 Let $a$ and $b$ be relatively prime integers and let $k$ be any integer. Show that $b$ and $a + bk$ are relatively prime.

**Solution:** Let $d = \gcd(b, a + bk)$. We will show that $d \mid 1$ and thus we must have that $d = 1$ (as $d$ is positive), concluding that $a$ and $a + bk$ are relatively prime.

Since $d \mid b$ and $d \mid a + bk$, we can write that $b = qd$ and $a + bk = q'd$ for some integers $q$ and $q'$. Thus $a + (qd)k = q'd$ and thus $a = (q' - qk)d$. Thus $d \mid a$.

Since $d$ divides both $a$ and $b$, it thus divides their gcd which is 1 (since $a$ and $b$ are relatively prime). Thus $d \mid 1$ and hence $d = 1$. \qed

#5 Suppose that $p \geq 2$ is an integer with the following property: if $m$ and $n$ are integers with $p \mid mn$, either $p \mid m$ or $p \mid n$. Show that $p$ must be a prime. (Hint: use a proof by contradiction.)

**Solution:** We will show this result by contradiction. Assume that $p$ is not prime; then we can write $p = ab$ where $1 < a < p$ and $1 < b < p$.

Since $p = ab$, $p \mid ab$. But by hypothesis, for any integers $m$ and $n$, if $p \mid mn$, then either $p \mid m$ or $p \mid n$. Thus $p \mid a$ or $p \mid b$; implying that $2 \leq p \leq a$ or $2 \leq p \leq b$. Therefore we have that $p \leq a < p$ or $p \leq b < p$; which are contradictions. Hence $p$ is prime. \qed