1. (a) The binary expansion of 20 is $20 = 16 + 4 = 2^4 + 0 \cdot 2^3 + 2 \cdot 2^2 + 0 \cdot 2^1 + 0 \cdot 2^0$, so here $r = 4$ and $i_1 = i_3 = i_4 = 0$, $i_2 = 1$. Thus, the power-mod algorithm runs as follows:

<table>
<thead>
<tr>
<th>$y_0$</th>
<th>$y_1$</th>
<th>$y_2$</th>
<th>$y_3$</th>
<th>$y_4$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$9 \equiv -4 \pmod{13}$</td>
<td>$y_0^2 a^{i_1} \equiv (-4)^2 \equiv 3 \pmod{13}$</td>
<td>$y_0^2 a^{i_2} \equiv 3^2 \equiv -4 \pmod{13}$</td>
<td>$y_3 \equiv y_0^2 a^{i_3} \equiv 3^2 \equiv -4 \pmod{13}$</td>
<td>$y_4 \equiv y_0^2 a^{i_4} \equiv (-4)^2 \equiv 3 \pmod{13}$</td>
</tr>
</tbody>
</table>

Thus, $\text{rem}(9^{20}, 13) = 3$.

(b) Similarly, since $13 = 8 + 5 = 8 + 4 + 1 = 2^3 + 1 \cdot 2^2 + 0 \cdot 2^1 + 1 \cdot 2^0$, we have here $r = 3$ and $i_1 = i_3 = 1$, $i_2 = 0$. Thus:

<table>
<thead>
<tr>
<th>$y_0$</th>
<th>$y_1$</th>
<th>$y_2$</th>
<th>$y_3$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$15 \equiv -3 \pmod{18}$</td>
<td>$y_0^2 a^{i_1} \equiv (-3)^2(-3) \equiv -27 \equiv 9 \pmod{18}$</td>
<td>$y_2 \equiv y_0^2 a^{i_2} \equiv 9^2 \equiv 9 \pmod{18}$</td>
<td>$y_3 \equiv y_0^2 a^{i_3} \equiv 9^2(-3) \equiv -27 \equiv 9 \pmod{18}$</td>
</tr>
</tbody>
</table>

Thus, $\text{rem}(15^{13}, 18) = 9$.

2. (a) Since $\gcd(3, 17) = 1$, the implication is true for all $x, y \in \mathbb{Z}$ by the Cancellation Law.

(b) This is false for $x = y = 5$. Indeed, $3x = 15 \equiv 0 \equiv 45 \equiv 9y \pmod{15}$, but $x = 5 \neq 3y = 15 \equiv 0 \pmod{15}$.

(c) If $2| x$, then $4|x^2$, so $x^2 \equiv 0 \pmod{4}$. If $x$ is odd, then $2|(x \pm 1)$, so $4|(x-1)(x+1) = x^2 - 1$, which means that $x^2 \equiv 1 \pmod{4}$. Thus in all cases $x^2 \equiv 0$ or 1 (mod 4), and the same is true for $y^2$. Therefore, $x^2 + y^2 \equiv 0$ or 1 or 2 (mod 4), so $x^2 + y^2 \not\equiv 3 \pmod{4}$, for any $x, y \in \mathbb{Z}$ or, equivalently, $x^2 + y^2 \not\equiv 4k + 3$, for any integers $x, y, k$.

4. (a) Since $\gcd(11, 57) = 1$, there is a unique solution (mod 57). To find it, solve $11x + 57y = 1$ using the Euclidean algorithm:

\[ 57 = 5 \cdot 11 + 2, \quad 11 = 5 \cdot 2 + 1, \]

so $1 = 11 - 5 \cdot 2 = 11 - 5(57 - 11 \cdot 5) = 11 \cdot 26 + 57(-5)$. Thus $x_0 = 26$ satisfies $11x_0 \equiv 1 \pmod{57}$ and hence $x = 23x_0 \equiv 23 \cdot 26 \equiv 28 \pmod{57}$ is the unique solution.

(b) Here $\gcd(12, 63) = 3$. Since $3 \not\mid 28$, the congruence equation has no solutions.

(c) Here $\gcd(16, 36) = 4$, and $4|40$, so there are precisely 4 solutions (mod 36). To find these, solve $16x + 36y = 4$. Since $36 = 2 \cdot 16 + 4$, we can take $x = -2$, $y = 1$. Thus, the formula gives $x = \frac{49}{4}(-2) + \frac{36}{4}t = -20 + 9t$, $t \in \mathbb{Z}$, so we get $x \equiv -20, -11, -2, 7 \pmod{36}$, or $x \equiv 7, 16, 25, 34 \pmod{36}$.

5. (a) The given equation is equivalent to the congruence equation $5x \equiv 2 \pmod{13}$. Since $\gcd(5, 13) = 1$, Theorem 4 tells us that this congruence equation has a unique solution. Since $5(8) = 40 \equiv 1 \pmod{13}$, we see that $x \equiv 2 \cdot 8 \equiv 3 \pmod{13}$. Thus, $x = [3]$ (or just $x = 3$) is the desired solution of the equation in $\mathbb{F}_{13}$.

(b) Here we have to solve $16x \equiv 40 \pmod{36}$. In part (c) of the previous question we found that there are four solutions: $x \equiv 7, 16, 25, 34 \pmod{36}$. Thus, the four solutions of $16x = 40$ in $\mathbb{Z}/36\mathbb{Z}$ are: $x = [7], [16], [25], [34]$ (or $x \equiv 7, 16, 25, 34$).

6. (a) Since $\gcd(m_1, m_2) = \gcd(27, 31) = 1$, we can apply the method of the Chinese Remainder Theorem. We have $m = 27 \cdot 31 = 837$, and

\[ m'_1 = \frac{27 \cdot 31}{27} = 31, \quad m'_1 \equiv 4 \pmod{27} \]
\[ m'_2 = \frac{27 \cdot 31}{31} = 27, \quad m'_2 \equiv -4 \pmod{31}. \]

We can find $m'_1$ by inspection \( \{ -4m'_1 \equiv 1 \pmod{27} \Rightarrow m'_1 \equiv 7 \pmod{27} \} \). (Indeed: \( 4 \cdot 7 \equiv 1 \pmod{27} \) and \( -4(-4)(-8) \equiv 1 \pmod{31} \).) Thus, since $a_1 = 11, a_2 = 13$, we get
\[ x \equiv a_1 m_1^* m_1' + a_2 m_2^* m_2' + a_3 m_3^* m_3' \pmod{m} \]
\[ \equiv 11 \cdot 7 \cdot 31 + 13 \cdot (-8) \cdot 27 \pmod{837} \]
\[ \equiv 2387 - 2808 \equiv -421 \equiv 416 \pmod{837}, \]

and so the solution is \( x \equiv 416 \pmod{837} \). (The answer \( x \equiv -421 \pmod{837} \) is also acceptable.)

(b) Here we have \( m_1 = 21 \), \( m_2 = 26 \), \( m_3 = 31 \). Since \( \gcd(21, 26) = \gcd(21, 31) = \gcd(26, 31) = 1 \), we can apply the CRT formula. (Note that checking the much weaker condition \( \gcd(21, 26, 31) = 1 \) is insufficient here.) We have \( m = 23 \cdot 27 \cdot 31 = 16926 \), and
\[
\begin{align*}
m_1' &= \frac{21 \cdot 26 \cdot 31}{21} = 26 \cdot 31, & m_1' &\equiv 5 \cdot 10 \equiv 8 \pmod{21} \\
m_2' &= \frac{21 \cdot 26 \cdot 31}{26} = 21 \cdot 31, & m_2' &\equiv (-5)5 \equiv 1 \pmod{26} \\
m_3' &= \frac{21 \cdot 26 \cdot 31}{31} = 21 \cdot 26, & m_3' &\equiv (-10)(-5) \equiv -12 \pmod{31}.
\end{align*}
\]

We now calculate the \( m_i^* \):
\[
\begin{align*}
8m_1^* &\equiv 1 \pmod{21} \Rightarrow m_1^* \equiv 8 \pmod{21} \\
m_2^* &\equiv 1 \pmod{26} \Rightarrow m_2^* \equiv 1 \pmod{26} \\
-12m_3^* &\equiv 1 \pmod{31} \Rightarrow m_3^* \equiv -13 \pmod{31}.
\end{align*}
\]

These are not so easy to do by inspection, so we use the extended Euclidean algorithm. We have \( 21 = 2 \cdot 8 + 5 \), \( 8 = 1 \cdot 5 + 3 \), \( 5 = 3 + 2 \), \( 3 = 2 + 1 \), so \( 1 = 3 - 2 = 2 \cdot 3 - 5 = 2 \cdot 8 - 3 \cdot 5 = 8 \cdot 8 - 3 \cdot 21 \). Thus, \( 8(8) - 3(21) = 1 \), and hence \( m_1^* \equiv 8 \pmod{21} \). Similarly, \( 31 = 2 \cdot 12 + 7 \), \( 12 = 7 + 5 \), \( 7 = 5 + 2 \), \( 5 = 2 \cdot 2 + 1 \), so \( 1 = 5 - 2(2) = 3(7) - 4(5) = 7(7) - 4(12) = 7(31) - 18(12) \). Thus, \( 7(31) - 18(12) = 1 \), and hence \( m_3^* \equiv 18 \equiv -13 \pmod{31} \).

Thus, since \( a_1 = 3 \), \( a_2 = -4 \), \( a_3 = 5 \), we get
\[
\begin{align*}
x &\equiv a_1 m_1^* m_1' + a_2 m_2^* m_2' + a_3 m_3^* m_3' \pmod{m} \\
&\equiv 3(8)(26 \cdot 31) + 4(1)(21 \cdot 31) + 5(-13)(21 \cdot 26) \pmod{16926} \\
&\equiv 19344 + 2604 - 35490 \equiv -13542 \equiv 3384 \pmod{16926},
\end{align*}
\]

and hence the solution is \( x \equiv 3384 \pmod{16926} \).