(1) Below are the primes up to 100, sorted by congruence class.

<table>
<thead>
<tr>
<th>Mod 9</th>
<th>Prime</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>19, 37, 73</td>
</tr>
<tr>
<td>1</td>
<td>2, 11, 29, 47, 83</td>
</tr>
<tr>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>3</td>
<td>13, 31, 67</td>
</tr>
<tr>
<td>4</td>
<td>5, 23, 41, 59</td>
</tr>
<tr>
<td>5</td>
<td>7, 43, 61, 79, 97</td>
</tr>
<tr>
<td>6</td>
<td>17, 53, 71, 89</td>
</tr>
</tbody>
</table>

There are at least two in each class except 0 mod 9, 3 mod 9, and 6 mod 9. In fact, these classes have no primes except 3 itself, because any such prime would satisfy \( p \equiv 0, 3, \text{ or } 6 \mod 3 \), i.e. \( p \equiv 0 \mod 3 \) and \( 3 \mid p \). So 3 is the only such prime.

(2) a) \( 55x \equiv 30 \mod 625 \)

\[ \Rightarrow 11x \equiv 6 \mod 125 \]

Using the Euclidean algorithm:

\[
\begin{align*}
\langle 4 \rangle &= (125) - 11 \cdot (11) \\
\langle 3 \rangle &= [11] - 2 \cdot \langle 4 \rangle = 23 \cdot (11) - 2 \cdot (125) \\
\langle 1 \rangle &= \langle 4 \rangle - \langle 3 \rangle = 3 \cdot (125) - 34 \cdot (11)
\end{align*}
\]

Hence \( -34 \cdot 11 \equiv 1 \mod 125 \). So

\[ x \equiv -34 \cdot 6 \mod 125 \]

i.e. \( x \equiv -204 \equiv 46 \).
so the solutions can be expressed either by

\[ x \equiv 46 \mod 125 \quad \text{or} \quad x \equiv 46, 171, 296, 421, \text{or} 546 \mod 625 \]

b) Since 11 divides 1331 and 55 but not 30, this congruence has [no solutions].

3 a) Suppose that \( y_1, y_2 \) are both inverses of \( x \) modulo 24. Then consider the number \( y_1 y_2 \). On the one hand

\[ y_1 y_2 \equiv y_1 \cdot (xy_2) \equiv y_1 \mod 24 \]

but on the other

\[ y_1 y_2 \equiv (y_1 x) y_2 \equiv y_2 \mod 24. \]

Hence \( y_1 \equiv y_2 \mod 24 \) (both are congruent to \( y_1 y_2 \)).

b) Notice that if \( xy \equiv 1 \mod 24 \), then \( \gcd(x, 24) \) must divide 1, hence \( \gcd(x, 24) = 1 \).

Conversely, if \( \gcd(x, 24) = 1 \), then the equation \( xy + 24z = 1 \) has a solution \((y, z)\), and \( y \) is an inverse of \( x \) modulo 24.

So \( x \) has an inverse if and only if \( \gcd(x, 24) = 1 \), i.e. if and only if \( x \) is not divisible by 2 or 3.

So we must find inverses for 5, 1, 5, 7, 11, 13, 17, 19, and 23.
Each can be found with the Euclidean algorithm.

\[
\begin{align*}
(24) & \quad (5) & (24) & \quad (7) \\
&= 5(5) - (24) & &= 7(7) - 2(24) \\
\text{so 5's inverse is 5.} & & \text{so 7's inverse is 7.}
\end{align*}
\]

\[
\begin{align*}
(24) & \quad (11) & (24) & \quad (13) \\
&= 11(11) - 5(24) & &= 2(13) - (24) \\
\text{so 11's inverse is 11.} & & \text{so 13's inverse is -11 (or 13).}
\end{align*}
\]

At this point, we can save some work by noticing that if

\[xy \equiv 1, \text{ then } (-x)(-y) = 1.\]

Since \(13 \equiv -11, 17 \equiv -7, \text{ and } -19 \equiv 5\) and \(23 \equiv -1,\) we can find the inverses from earlier work. Note

\[
\begin{array}{cccccccccc}
\times & 1 & 5 & 7 & 11 & 13 & 17 & 19 & 23 \\
\hline
1 & 1 & 5 & 7 & 11 & 13 & 17 & 19 & 23 \\
\text{inverse} & 1 & 5 & 7 & 11 & 13 & 17 & 19 & 23 \\
\end{array}
\]

So \(\text{mod} 24\) arithmetic has a strange property: each invertible element is its own inverse.
(4) a) Let \( L = \text{lcm}(a,b) \). Suppose \( \gcd(a,b) = 1 \). Then for some \( x, y \),

\[
ax + by = 1
\]

\[
\Rightarrow axL + byL = L
\]

\[
\Rightarrow L = ab \cdot (x \cdot \frac{1}{b} + y \cdot \frac{1}{a})
\]

so \( L \) is a multiple of \( ab \). Since \( ab \) is a common multiple of \( a \) & \( b \), it can't be strictly smaller than \( L \); hence \( L = ab \).

b) Suppose that \( N \) is a common multiple of \( ka \) and \( kb \).
Then \( \frac{N}{k} \) is divisible by both \( a \) and \( b \). Hence \( \frac{N}{k} \) is a common multiple of \( a \) and \( b \), so \( N/k \geq \text{lcm}(a,b) \), so \( N = k \cdot \text{lcm}(a,b) \). This shows that if \( k \cdot \text{lcm}(a,b) \) is a common multiple of \( ka \) and \( kb \), then it must necessarily be the least one.

Now, \( k \cdot \text{lcm}(a,b)/(ka) = \text{lcm}(a,b)/a \) and \( k \cdot \text{lcm}(a,b)/(kb) = \text{lcm}(a,b)/b \), so \( k \cdot \text{lcm}(a,b) \) is a common multiple of \( ka \) & \( kb \). By the previous paragraph, it is equal to the least common multiple.

c) Let \( g = \gcd(a,b) \). Then \( \gcd\left(\frac{a}{g}, \frac{b}{g}\right) = 1 \) since \( \frac{a}{g} x + \frac{b}{g} y = 1 \) has a solution. By part (a), \( \text{lcm}(\frac{a}{g}, \frac{b}{g}) = \frac{ab}{g^2} \).
So by part (b),

\[
\text{lcm}(a,b) = g \cdot \text{lcm}(\frac{a}{g}, \frac{b}{g}) = g \cdot \frac{ab}{g^2} = \frac{ab}{g}.
\]

Therefore, \( g \cdot \text{lcm}(a,b) = ab \), as claimed.
The numbers \((a, b, c^2)\) must be a primitive Pythagorean triple. So we want integers \(s, t\), odd and with no common factor, such that

\[
\begin{align*}
a &= st \\
b &= \frac{1}{2}(s^2 - t^2) \\
c^2 &= \frac{1}{2}(s^2 + t^2)
\end{align*}
\]

i.e., \(2c^2 = s^2 + t^2\).

Using \(PSet2\), problem 3(b), one option is \(s = 7, t = 1\), since then \(c = 5\) gives \(2c^2 = s^2 + t^2\).

So \(a = 7, b = 24, c = 5\) is one solution.

Other solutions to the eqn. \(2c^2 = s^2 + t^2\) from \(HW2\) give more solutions to \(a^2 + b^2 = c^4\). For example,

\[
2 \cdot 13^2 = 17^2 + 7^2
\]

gives the solution \(s = 17, t = 7\), hence values

\[
\begin{align*}
a &= 17 \cdot 7 = 119 \\
b &= \frac{1}{2}(17^2 - 7^2) = 120 \\
c &= \frac{1}{2}(17^2 + 7^2) = 13
\end{align*}
\]

is another solution.