Show all of your work.

1. What are the elements of $\mathbb{Z}_{21}$?

   **Solution:** Start with $0, \ldots, 20$ and strike out the classes of integers not relatively prime to 21. What’s left is $1, 2, 4, 5, 8, 10, 13, 16, 17, 19, 20$. As a check, notice that $\phi(21) = \phi(3) \cdot \phi(7) = 2 \cdot 6 = 12$. Thus, there are 12 units in $\mathbb{Z}_{21}$.

2. What is $\phi(18,000)$?

   **Solution:**
   
   $\phi(18,000) = \phi(2^4 \cdot 3^2 \cdot 5^3) = \phi(2^4) \cdot \phi(3^2) \cdot (5^3)$
   
   $= 2^3(2 - 1) \cdot 3^1(3 - 1) \cdot 5^2(5 - 1) = 4800$.

3. a) What are the possible orders of the elements of $\mathbb{Z}_{125}^\times$?

   **Solution:** The possible orders are the divisors of $\phi(125) = \phi(5^3) = 100$ (as in the last problem). Thus the order of an element may be 1, 2, 4, 5, 10, 20, 25, 50, or 100.

   b) What is the order of $21$ in $\mathbb{Z}_{125}^\times$?

   **Solution:** Testing the possible orders using maple, we see that $21^2 = \overline{66}, 21^4 = \overline{106}, 21^5 = \overline{101}, 21^{10} = \overline{76}, 21^{20} = \overline{26}, 21^{25} = \overline{1}$. Thus, $21$ has order 25 in $\mathbb{Z}_{125}^\times$.

   c) What is the smallest positive integer congruent to $21^{78252347380}$ mod 125?

   **Solution:** We see immediately that $78252347380 \equiv 5 \mod 25$, and hence $78252347380 = 25q + 5$ for some $q$. Thus, $21^{78252347380} = (21^{25})^q \cdot 21^5 \equiv 1^q \cdot 21^5 \equiv 101 \mod 25$.

   The congruences $21^{25} \equiv 1$ and $21^5 \equiv 101$ were shown in part b).
4. What is the order of $2^{71186259842}$ in $\mathbb{Z}_{17}^\times$?

**Solution:** We first calculate the order of $2$. The possible orders are the divisors of $\phi(17) = 16$, i.e., 1, 2, 4, 8, and 16. We have $2^2 = 4, 2^4 = 16$, and $2^8 = 1$, so 2 has order 8. Thus, the order of $2^k$ is $\frac{8}{(8,k)}$ for any $k$. Now, $(8, 71186259842) = 2$, so $2^{71186259842}$ has order $\frac{8}{2} = 4$.

5. For which primes $p$ is $x^{41} \equiv x \pmod{p}$ for all $x \in \mathbb{Z}$?

**Solution:** Our theorem tells us that $x^k \equiv x \pmod{p}$ for all $x \in \mathbb{Z}$ if and only if $k \equiv 1 \pmod{p-1}$. We have:

<table>
<thead>
<tr>
<th>$p$</th>
<th>$p-1$</th>
<th>$41 \pmod{p-1}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>1</td>
<td>0 $\equiv$ 1</td>
</tr>
<tr>
<td>3</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>5</td>
<td>4</td>
<td>1</td>
</tr>
<tr>
<td>7</td>
<td>6</td>
<td>5</td>
</tr>
<tr>
<td>11</td>
<td>10</td>
<td>1</td>
</tr>
<tr>
<td>13</td>
<td>12</td>
<td>5</td>
</tr>
<tr>
<td>17</td>
<td>16</td>
<td>9</td>
</tr>
<tr>
<td>19</td>
<td>18</td>
<td>5</td>
</tr>
<tr>
<td>23</td>
<td>22</td>
<td>19</td>
</tr>
<tr>
<td>29</td>
<td>28</td>
<td>13</td>
</tr>
<tr>
<td>31</td>
<td>30</td>
<td>11</td>
</tr>
<tr>
<td>37</td>
<td>36</td>
<td>5</td>
</tr>
<tr>
<td>39</td>
<td>38</td>
<td>3</td>
</tr>
<tr>
<td>41</td>
<td>40</td>
<td>1</td>
</tr>
</tbody>
</table>

Thus, the primes that satisfy the theorem are 2, 3, 5, 11, 41.
6. Find the smallest nonnegative solution for the following congruences.

\[ x \equiv 96 \mod 120 \]
\[ x \equiv 48 \mod 54 \]
\[ x \equiv 51 \mod 75 \]

**Solution:** We begin by solving the first two congruences:

\[ 96 + 120r = 48 + 54s \]
\[ 48 = 96 - 48 = 120(-r) + 54s \]

Solving Bezout’s identity for 120 and 54, we have

\[ 120 = 2 \cdot 54 + 12 \]
\[ 54 = 4 \cdot 12 + 6, \]

so the gcd is 6, and we get

\[ 6 = 54 - 4 \cdot (120 - 2 \cdot 54) = -4 \cdot 120 + 9 \cdot 54. \]

Thus,

\[ 48 = 8 \cdot 6 = -32 \cdot 120 + 72 \cdot 54. \]

Thus, we may take \( r = 32 \) and \( s = 72 \), so

\[ x \equiv 96 + 32 \cdot 120 \mod [120, 54] \]
\[ \equiv 696 \mod 1080. \]

We now solve this last congruence together with \( x \equiv 51 \mod 75 \):

\[ 696 + 1080k = 51 + 75l \]
\[ 645 = 696 - 51 = 1080(-k) + 51l. \]

We again solve Bezout’s identity:

\[ 1080 = 14 \cdot 75 + 30 \]
\[ 75 = 2 \cdot 30 + 15, \]

so 15 is the gcd, and

\[ 15 = 75 - 2 \cdot (1080 - 14 \cdot 75) = -2 \cdot 1080 + 29 \cdot 75. \]

Thus,

\[ 645 = 43 \cdot 15 = -86 \cdot 1080 + 1247 \cdot 75. \]
Exam 2 Solutions

We may take $k = 86$ and $l = 1247$, hence

$$x \equiv 696 + 86 \cdot 1080 \mod [1080, 75]$$

$$\equiv 1776 \mod 5400.$$ 

So 1776 is the smallest non-negative solution of the original three congruences.

7. Find all solutions of $x^2 \equiv 1$ in

a) $\mathbb{Z}_{128}$

**Solution:** Our theorem says $x^2 \equiv 1$ in $\mathbb{Z}_{2^r}$ if and only if $x \equiv 1 \mod 2^{r-1}$. Here, $128 = 2^7$, so $r = 7$, and the solutions are $1$, $2^6 - 1 = 63$, $2^6 + 1 = 65$, $2^7 - 1 = 127$.

b) $\mathbb{Z}_{45}$

**Solution:** The prime decomposition of 45 is $9 \cdot 5$. Recall that if $p$ is an odd prime and $r > 0$, then $x^2 \equiv 1 \mod p^r$ if and only if $x \equiv \pm 1 \mod p^r$. The Chinese Remainder Theorem gives

$$x^2 \equiv 1 \mod 45 \iff x^2 \equiv 1 \mod 9$$

$$x^2 \equiv 1 \mod 5$$

$$\iff x \equiv \pm 1 \mod 9$$

$$x \equiv \pm 1 \mod 5$$

We list off the integers between 0 and 44 congruent to $\pm 1 \mod 9$ and calculate their congruence class mod 5:

<table>
<thead>
<tr>
<th>$x$</th>
<th>1</th>
<th>8</th>
<th>10</th>
<th>17</th>
<th>19</th>
<th>26</th>
<th>28</th>
<th>35</th>
<th>37</th>
<th>44</th>
</tr>
</thead>
<tbody>
<tr>
<td>$x \mod 5$</td>
<td>1</td>
<td>3</td>
<td>0</td>
<td>2</td>
<td>-1</td>
<td>1</td>
<td>3</td>
<td>0</td>
<td>2</td>
<td>-1</td>
</tr>
</tbody>
</table>

Thus, the solutions are $\bar{x} = 1$, $\bar{x} = 19$, $\bar{x} = 26$, and $\bar{x} = 44$. 

c) $\mathbb{Z}_{80}$:

**Solution**: Here, $80 = 2^4 \cdot 5$. We have

\[ x^2 \equiv 1 \mod 80 \iff x^2 \equiv 1 \mod 16 \]
\[ x^2 \equiv 1 \mod 5 \]
\[ \iff x \equiv \pm 1 \mod 8 \]
\[ x \equiv \pm 1 \mod 5 \]

Since $x \equiv \pm 1 \mod 8$, $x$ is odd. We list off the odd numbers between 0 and 79 congruent to $\pm 1 \mod 5$, and calculate their congruence class mod 8:

<table>
<thead>
<tr>
<th>$x$</th>
<th>1</th>
<th>9</th>
<th>11</th>
<th>19</th>
<th>21</th>
<th>29</th>
<th>31</th>
<th>39</th>
</tr>
</thead>
<tbody>
<tr>
<td>$x \mod 8$</td>
<td>1</td>
<td>1</td>
<td>3</td>
<td>3</td>
<td>5</td>
<td>5</td>
<td>-1</td>
<td>-1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>$x$</th>
<th>41</th>
<th>49</th>
<th>51</th>
<th>59</th>
<th>61</th>
<th>69</th>
<th>71</th>
<th>79</th>
</tr>
</thead>
<tbody>
<tr>
<td>$x \mod 8$</td>
<td>1</td>
<td>1</td>
<td>3</td>
<td>3</td>
<td>5</td>
<td>5</td>
<td>-1</td>
<td>-1</td>
</tr>
</tbody>
</table>

Thus, the solutions are $x = 1$, $x = 9$, $x = 31$, $x = 39$, $x = 41$, $x = 49$, $x = 71$, and $x = 79$. 