1. (3pts) Define the Euler's function $\phi(n)$.

   $\phi(n)$ is the number of integers between 1 and $n$ which are relatively prime to $n$.

2. (3pts) Find $\phi(15)$ using the definition of $\phi(n)$.

   1, 2, 4, 7, 8, 11, 13, 14 are the numbers between 1 and 15 and are relatively prime to 15. So $\phi(15) = 8$.

3. (4pts) State the multiplicative property of $\phi(n)$.

   If $m, n$ are relatively prime then $\phi(mn) = \phi(m) \phi(n)$.

4. (3pts) Compute $\phi(125)$.

   $125 = 5^3$, so $\phi(125) = 5^3 - 5^2 = 125 - 25 = 100$.

5. (3pts) Compute $\phi(1,000,000)$.

   $\phi(1,000,000) = \phi(10^6) = \phi(2^6, 5^6) = \phi(2^6) \phi(5^6) = 2^5 \cdot 5^5 (5-1) = 10^5 \cdot 4 = 400,000$.

6. (4pts) State Euler's Theorem.

   If $(a, n) = 1$ then $a^{\phi(n)} \equiv 1 \pmod{n}$.

7. (4pts) State Fermat's Theorem.

   If $p$ is a prime and $p \nmid a$ then $a^{p-1} \equiv 1 \pmod{p}$. 

Name:
8) (4pts) Derive Fermat’s Theorem from Euler’s Theorem.

(Assume Euler’s Theorem true and prove Fermat’s.)

If \( p \) is a prime then \( \phi(p) = p - 1 \)

Also if \( p \nmid a \) then \( (p, a) = 1 \)

So by Euler’s Theorem \( a^{\phi(p)} \equiv 1 \pmod{p} \)

\[ 9) \text{(5pts) Find the last two digits of } 7^{2011}. \text{ Show your work.} \]

We need to compute \( 7^{2011} \pmod{100} \)

Since \( \phi(100) = \phi(4 \cdot 25) = \phi(4) \phi(25) \)

\[ = 2, 5(5-1) = 40 \]

and \( 2011 = 50 \times 40 + 11 \)

\[ 7^{2011} = (7^{40})^{50} \cdot 7^{11} \]

\[ 7^{2011} \equiv 1^{50} \cdot 7^{11} \pmod{100} \]

by Euler’s Theorem

\[ 7^{2011} \equiv 7^{11} \pmod{100} \]

\[ 7^1 \equiv 7 \pmod{100} \]

\[ 7^2 \equiv 49 \pmod{100} \]

\[ 7^4 = (7^2)^2 \equiv 49^2 \equiv 49 \pmod{100} \]

\[ 7^8 \equiv (7^4)^2 \equiv 1 \pmod{100} \]

\[ 7^{11} \equiv 7^8 \cdot 7^2 \cdot 1 \equiv 49 \cdot 49 \cdot 1 \equiv 43 \pmod{100} \]

The last two digits of \( 7^{2011} \) are \( 43 \)
1) (5pts) State the Chinese Remainder Theorem.

If \( m_1, m_2, \ldots, m_k \) are pairwise relatively prime, then the system of congruences

\[
\begin{align*}
    x &\equiv a_1 \pmod{m_1} \\
    x &\equiv a_2 \pmod{m_2} \\
    &\vdots \\
    x &\equiv a_k \pmod{m_k}
\end{align*}
\]

has a solution. The solution is unique \( \mod{m_1 m_2 \cdots m_k} \).

2) (15pts) Find the smallest positive integer and the smallest three digit positive integer such that all congruences below hold simultaneously.

\[
\begin{align*}
    x &\equiv 2 \pmod{3} \\
    x &\equiv 2 \pmod{5} \\
    x &\equiv 4 \pmod{7}
\end{align*}
\]

Let \( M = 3 \cdot 5 \cdot 7 = 105 \)

\[
M_1 = \frac{M}{3} = 5 \cdot 7 = 35
\]

\( y_1 \) be defined by \( M_1 y_1 \equiv 1 \pmod{3} \)

\[
3 \cdot 5 y_1 \equiv 1 \pmod{3}
\]

\[
2 \cdot 5 y_1 \equiv 1 \pmod{3} \Rightarrow y_1 \equiv 2 \pmod{3}
\]

\[
M_2 = \frac{M}{5} = 3 \cdot 7 = 21 ; \quad M_2 y_2 \equiv 1 \pmod{5}
\]

\[
2 \cdot 1 y_2 \equiv 1 \pmod{5}
\]

so \( y_2 \equiv 1 \pmod{5} \)

\[
M_3 = \frac{M}{7} = 3 \cdot 5 = 15 ; \quad M_3 y_3 \equiv 1 \pmod{7}
\]

\[
15 y_3 \equiv 1 \pmod{7}
\]

\[
y_3 \equiv 1 \pmod{7}
\]

\[
x = 2 \cdot 35 + 2 \cdot 1 \cdot 121 + 4 \cdot 1 \cdot 15 = 140 + 42 + 60 = 242
\]

\[
242 \equiv 32 \pmod{105}
\]

\[
242 \equiv 32 + 105 = 137 \pmod{105}
\]

\( \boxed{32} \) is the smallest solution

\( \boxed{137} \) is the smallest 3-digit solution
1) (3pts) Define disjoint permutations. The permutation $\pi$ and $\sigma$ are disjoint if every element moved by $\pi$ is fixed by $\sigma$ and every element moved by $\sigma$ is fixed by $\pi$.

2) (6pts) State two properties of disjoint permutations.

- If $\pi$, $\sigma$ are disjoint then $\pi\sigma = \sigma\pi$

- If $\pi$, $\sigma$ are disjoint then

$$\text{order } (\pi\sigma) = \text{lcm}\left(\text{order}(\pi), \text{order}(\sigma)\right)$$

3) (6pts) Give an example of two permutations in $S(5)$ which are not disjoint. Check whether the properties you stated in III 2) hold for these permutations.

Let $\pi = (12)$
$\sigma = (25)$
$\pi\sigma = (125)$
$\sigma\pi = (152)$

$\neq \pi\sigma$

$\sigma$, $\pi$ do not commute

4) Let $\pi = (1, 2, 5, 9)(2, 4, 6)(4, 6, 7, 8)(3, 5)$

a) (3pts) Write $\pi$ as a product of disjoint cycles.

$$\pi = (124539)(678)$$
b) (4pts) Find the order of \( \pi \). Justify your answer.

\[
\begin{align*}
\text{ord} (124539) &= 6 \\
\text{ord} (678) &= 3 \\
\text{ord}(\pi) &= \text{lcm}(6, 3) = 6
\end{align*}
\]

c) (3pts) Find the sign of \( \pi \). Justify your answer.

\[
\begin{align*}
\text{Sign} (\pi) &= \text{Sign} (124539) \text{ Sign} (678) \\
&= (-1)^{6-1} (-1)^{3-1} = (-1)^5 (-1)^2 = -1 \cdot 1 = [-1]
\end{align*}
\]

\[\Pi\text{ is an odd permutation.}\]

IV Let \( S = \{1, 2, 3, \ldots, 20\} \) and let the operation \( \ast \) be defined on \( S \) by:

\[a \ast b = \text{minimum } (a, b)\]

1. (2pts) Is \( S \) closed under \( \ast \)?

Yes: the min of 2 numbers is one of them and is therefore in \( S \).

2. (2pts) Is \( \ast \) associative?

Yes \( a \ast (b \ast c) = (a \ast b) \ast c = \text{smallest of } (a, b, c) \).

3. (3pts) Does \( \ast \) have an identity? If no explain. If yes give that identity.

Yes \( \text{For all } x \in S \quad x \ast 20 = \text{min}(x, 20) = x \). 20 is an identity.

4. (5pts) Is \( S, \ast \) a group? a semigroup? Justify your answers.

Since \( S \) satisfies closure and associativity it is a semigroup (with identity).

However, if \( a < 20 \) there is no \( b \) such that

\[a \ast b = \min(a, b) = 20\text{ since } \min(a, b) \leq a < 20\]

So the inverse property does not hold. \( S \) is not a group.
Bob wants to receive encrypted messages using the RSA public key cryptosystem. Bob chooses two primes $p = 13$, $q = 37$ and publishes his encrypting modulus $n = pq$.

a) (5pts) Can Bob choose $e_1 = 9$ as his public encrypting exponent? Justify your answer.

$$\phi(n) = \phi(13) \phi(37) = 12 \cdot 36 = 432$$

$$\left(q, \phi(n)\right) = 9 \neq 1$$

So 9 is not relatively prime to $\phi(n)$.

It cannot be an encrypting exponent.

b) (10pts) Bob chooses $e = 25$ as his public encrypting exponent. Compute the decoding exponent $d$.

We need to solve $ed \equiv 1 \pmod{\phi(n)}$

$$25d \equiv 1 \pmod{432}$$

Let us use the Euclidian algorithm to compute $\gcd(432, 25)$

<table>
<thead>
<tr>
<th></th>
<th></th>
<th>432</th>
<th>25</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
<td>1</td>
<td>17</td>
</tr>
<tr>
<td>0</td>
<td></td>
<td>1</td>
<td>25</td>
</tr>
<tr>
<td>1</td>
<td></td>
<td>-17</td>
<td>7</td>
</tr>
<tr>
<td>-3</td>
<td></td>
<td>52</td>
<td>4</td>
</tr>
<tr>
<td>4</td>
<td></td>
<td>-69</td>
<td>3</td>
</tr>
<tr>
<td>-7</td>
<td></td>
<td>121</td>
<td>1</td>
</tr>
</tbody>
</table>

$\gcd(432, 25) = 1$

$$-7 \cdot 432 + 121 \cdot 25 = 1$$

$$121 \cdot 25 \equiv 1 \pmod{432}$$

$$d \equiv 121 \pmod{432}$$

The decoding exponent is $d = 121$.

c) (5pts) Alice sends Bob an encrypted message. The plain text is $P = 3$. What is the cipher text $C$?

$$C = 3^{25} \pmod{n} = 3^{25} \pmod{481}$$

$$3^2 = 9$$

$$3^4 = 81$$

$$3^8 \equiv 308 \pmod{481}$$

$$3^{16} \equiv 107$$

$$3^{25} \equiv 3^{16} \cdot 3^8 \equiv 308 \cdot 107 \cdot 3 \equiv 263 \pmod{481}$$

$$P = 263$$