Name (please be legible) ________________________________
Preferred name ________________________________
Student number ________________________________

INSTRUCTIONS

• Duration: 50 minutes
• This test has 4 problems for a total of 100 points.
• This test has 5 pages including this one.
• Read all the questions carefully before starting to work.
• For problems with several parts indicate clearly which part of it you are answering.
• You should give complete arguments and explanations for all your claims and calculations; answers without justifications will not be marked.
• You may write on the backs of pages if you run out of space.
• Attempt to answer all questions for partial credit.
• This is a closed-book examination. None of the following are allowed: documents, cheat sheets or electronic devices of any kind (including calculators, cell phones, etc.)

<table>
<thead>
<tr>
<th>Question:</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Points:</td>
<td>25</td>
<td>25</td>
<td>30</td>
<td>20</td>
<td>100</td>
</tr>
<tr>
<td>Score:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
PROBLEM 1 (25 points)

Decide if the following statements are TRUE or FALSE. If a statement
is TRUE give a proof and if a statement is FALSE give an example where
it fails. Answering only TRUE or FALSE is worth ZERO points.

Let $\phi$ denote the Euler $\phi$-function.

Let $a, b, c, m \in \mathbb{Z}$ with $m > 0$.

(a) (5pts) If $\phi(m) = m - 1$ then $m$ is prime.

Answer: True.

We have $\phi(m) \leq m - 1$ by definition of the function $\phi$. If $m$ is not
prime then $m = ab$ with $1 < a, b < m$ and clearly $(m, a) = a > 1$.
Thus $\phi(m) \leq m - 2$ because the integer $a$ is not counted by $\phi$.

(b) (5pts) If $a \equiv b \pmod{m}$ then $c^a \equiv c^b \pmod{m}$.

Answer: False.

We have $6 \equiv 3 \pmod{3}$ but $2^3 \equiv 2 \not\equiv 1 \equiv 2^6 \pmod{3}$.

(c) (5pts) If $a > 0$ is odd then $\phi(2a) = \phi(a)$.

Answer: True.

Note that $\phi(2) = 1$. We have $(2, a) = 1$ because $a$ is odd and since
$\phi$ is multiplicative it follows $\phi(2a) = \phi(2)\phi(a) = \phi(a)$.

(d) (5pts) If $a^2 \equiv 1 \pmod{m}$ then $a \equiv \pm 1 \pmod{m}$.

Answer: False.

Take $a = 3$ and $m = 8$. We have $3^2 = 9 \equiv 1 \pmod{8}$ but $3 \not\equiv \pm 1$
(mod 8).

(e) (5pts) The integer 723160823 is divisible by 11.

Answer: True.

Let $N = 723160823$. The alternate sum of the digits of $N$ is $S =
7 - 2 + 3 - 1 + 6 - 0 + 8 - 2 + 3 = 22$. Since $11 \mid S$ we conclude by the
criterion for divisibility by 11 that $11 \mid N$. 
PROBLEM 2 (25 points)

Let \( \phi \) be the Euler \( \phi \)-function. Find all positive integers \( n \) such that \( \phi(n) = 4 \). You can use the following fact in your proof.

**FACT:** If \( m \in \mathbb{Z}_{>0} \) satisfies \( \phi(m) = 2 \) then \( m = 3, 4 \) or 6.

**Answer:** Suppose \( \phi(n) = 4 \). Thus \( n > 1 \) because \( \phi(1) = 1 \).

Let \( n = p_1^{a_1} \cdots p_k^{a_k} \), \( a_i \geq 1 \) be the prime decomposition of \( n \).

Recall that

\[
\phi(p_i^{a_i}) = p_i^{a_i - 1}(p_i - 1) \quad \text{and} \quad \phi(n) = \phi(p_1^{a_1}) \cdots \phi(p_k^{a_k}).
\]

We see that \( p_i - 1 \mid 4 \) for each prime factor of \( n \), i.e. \( p_i - 1 \in \{1, 2, 4\} \), hence \( p_i = 2, 3 \) or 5. We conclude that \( n \) is of the form

\[
n = 2^a \cdot 3^b \cdot 5^c, \quad a, b, c \geq 0.
\]

If \( b \geq 2 \) then \( 3 \mid \phi(n) = 4 \) a contradiction; thus \( b = 0 \) or \( b = 1 \). We now divide into two cases:

1. Suppose \( b = 1 \). Then \( n = 2^a \cdot 3 \cdot 5^c \) and

\[
4 = \phi(n) = \phi(3)\phi(2^a5^c) = 2\phi(2^a5^c),
\]

hence \( \phi(2^a5^c) = 2 \). From the fact we have \( 2^a5^c = 3, 4, 6 \) which is only possible when \( a = 2 \) and \( c = 0 \), that is \( n = 12 \).

2. Suppose \( b = 0 \). Then \( n = 2^a \cdot 5^c \).

We have \( c = 0 \) or \( c = 1 \) otherwise \( 5 \mid \phi(n) = 4 \).

If \( c = 1 \) then \( n = 2^a \cdot 5 \) and \( \phi(n) = 4\phi(2^a) = 4 \) implies \( \phi(2^a) = 1 \); thus \( a = 0, 1 \) that is \( n = 5, 10 \).

If \( c = 0 \) then \( n = 2^a \) and \( \phi(2^a) = 4 \) implies \( a = 3 \) that is \( n = 8 \).

The complete set of solutions is \( n = 5, 8, 10, 12 \).
PROBLEM 3 (30 points)

(a) (5pts) State the Chinese Remainder Theorem.

Answer: Let \(n_1, n_2, \ldots, n_k \in \mathbb{Z}_{>0}\) and pairwise coprime. Let \(b_1, b_2, \ldots, b_k \in \mathbb{Z}\). Then the system of congruences

\[
\begin{align*}
  x &\equiv b_1 \pmod{n_1} \\
  x &\equiv b_2 \pmod{n_2} \\
  &\vdots \\
  x &\equiv b_k \pmod{n_k}
\end{align*}
\]

has a unique solution modulo \(M = n_1 \cdot n_2 \cdot \ldots \cdot n_k\).

(b) (25pts) Compute \(8^{10003} \pmod{105}\) using the Chinese remainder theorem. Note that \(105 = 3 \cdot 5 \cdot 7\).

Answer: We have to find an integer \(x\) such that

\[x \equiv 8^{10003} \pmod{105}, \quad 0 \leq x \leq 104.\]

Note that \(105 = 3 \cdot 5 \cdot 7\). The value of \(x\) will also satisfy the system of congruences

\[x \equiv 8^{10003} \pmod{3}, \quad x \equiv 8^{10003} \pmod{5}, \quad x \equiv 8^{10003} \pmod{7},\]

which we will solve by using CRT. We first simplify the congruences above. Note that

\[8 \equiv -1 \pmod{3}, \quad 8 \equiv -2 \pmod{5}, \quad 8 \equiv 1 \pmod{7}\]

can be rewritten as

\[
\begin{align*}
  x &\equiv (-1)^{10003} \equiv -1 \pmod{3} \\
  x &\equiv (-2)^{10003} \pmod{5}, \\
  x &\equiv 1^{10003} \equiv 1 \pmod{7}.
\end{align*}
\]

To compute \((-2)^{10003} \pmod{5}\) we note that \((-2)^4 = 16 \equiv 1 \pmod{5}\) which implies

\[x \equiv (-2)^{10003} \equiv ((-2)^4)^{2500} \cdot (-2)^3 \equiv 1 \cdot (-8) \equiv 2 \pmod{5}.
\]

We conclude that we want to use CRT with the system of congruences

\[
\begin{align*}
  x &\equiv -1 \pmod{3} \\
  x &\equiv 2 \pmod{5}, \\
  x &\equiv 1 \pmod{7}.
\end{align*}
\]

That is \(M = 3 \cdot 5 \cdot 7 = 105\), \(M_1 = 35\), \(M_2 = 21\), \(M_3 = 15\), \(n_1 = 3\), \(n_2 = 5\), \(n_3 = 7\), \(b_1 = -1\), \(b_2 = 2\) and \(b_3 = 1\).

Finally, we have to find solutions \(y_i\) to the congruences \(M_i x \equiv 1 \pmod{n_i}\) that is

\[
\begin{align*}
  35x &\equiv 2x \equiv 1 \pmod{3}, \\
  21x &\equiv x \equiv 1 \pmod{5}, \\
  15x &\equiv x \equiv 1 \pmod{7}
\end{align*}
\]
we can take \( y_1 = -1 \), and \( y_2 = y_3 = 1 \). The value of \( x \) \( \text{mod} \) 105 can now be computed by
\[
x \equiv b_1 M_1 y_1 + b_2 M_2 y_2 + b_3 M_3 y_3 \equiv 35 + 42 + 15 \equiv 92 \pmod{105}.
\]

**Alternative I:** Since \(-1 \equiv 2 \pmod{3}\) by CRT we can rewrite the system (1) as
\[
\begin{align*}
x &\equiv 2 \pmod{15} \\
x &\equiv 1 \pmod{7}
\end{align*}
\]
and apply CRT to it. Indeed, \( M = 15 \cdot 7 = 105 \), \( M_1 = 7 \), \( M_2 = 15 \)
\( n_1 = 15 \), \( n_2 = 7 \), \( b_1 = 2 \) and \( b_2 = 1 \). We need solutions \( y_i \) to the congruences \( M_i x \equiv 1 \pmod{n_i} \), that is
\[
7x \equiv 1 \pmod{15}, \quad 15x \equiv 1 \pmod{7},
\]
hence we can take \( y_1 = -2 \), and \( y_2 = 1 \). The value of \( x \) \( \text{mod} \) 105 can now be computed by
\[
x \equiv b_1 M_1 y_1 + b_2 M_2 y_2 \equiv 2 \cdot 7 \cdot (-2) + 1 \cdot 15 \cdot 1 \equiv 92 \pmod{105}.
\]

**Alternative II:** Using FLT and/or direct calculations, we check that
\[
8^2 \equiv 1 \pmod{3}, \quad 8^4 \equiv 1 \pmod{5}, \quad 8 \equiv 1 \pmod{7}.
\]
Since 10000 is a multiple of 2 and 4 we conclude that
\[
\begin{align*}
8^{10000} &\equiv 1 \pmod{3} \\
8^{10000} &\equiv 1 \pmod{5} \\
8^{10000} &\equiv 1 \pmod{7},
\end{align*}
\]
hence it follows from CRT that
\[
8^{10000} \equiv 1 \pmod{105}.
\]
Therefore,
\[
x = 8^{10003} = 8^{10000} \cdot 8^3 \equiv 1 \cdot 512 \equiv 92 \pmod{105}.
\]
PROBLEM 4 (20 points)

Suppose that \( n \in \mathbb{Z}_{>0} \) has 77 positive divisors. How many of these divisors can be primes?

**Answer:** Let \( n = p_1^{a_1} \cdots p_k^{a_k}, \ a_i \geq 1 \) be the prime decomposition of the positive integer \( n \).

We know that the number of positive divisors of \( n \) is \( \tau(n) = 77 \) and it is also given by
\[
\tau(n) = (a_1 + 1) \cdots (a_k + 1) = 77.
\]

The positive divisors of 77 are \( \{1, 7, 11, 77\} \).

Suppose \( a_1 + 1 = 77 \). Then \( a_i = 0 \) for all \( i \geq 2 \). Thus \( n = p_1^{76} \).

Suppose \( a_1 + 1 = 11 \). Then \((a_2 + 1) \cdots (a_k + 1) = 7\) which implies \( a_2 = 6 \) and \( a_i = 0 \) for all \( i \geq 3 \). Thus \( n = p_1^{10} p_2^6 \).

Suppose \( a_1 + 1 = 7 \). Then \((a_2 + 1) \cdots (a_k + 1) = 11\) which implies \( a_2 = 10 \) and \( a_i = 0 \) for all \( i \geq 3 \). Thus \( n = p_1^6 p_2^{10} \).

Suppose \( a_1 + 1 = 1 \). Hence \( a_1 = 0 \) which contradicts \( a_1 \geq 1 \).

Thus \( n \) has either 1 or 2 prime factors.