Name (please be legible) ________________________________
Signature __________________________________________
Student number ________________________________

INSTRUCTIONS

- **Duration:** 90 minutes
- This test has 7 problems for a total of 100 points.
- This test has 8 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>5</th>
<th>6</th>
<th>7</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Points:</td>
<td>10</td>
<td>10</td>
<td>10</td>
<td>15</td>
<td>15</td>
<td>20</td>
<td>20</td>
<td>100</td>
</tr>
<tr>
<td>Score:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Score: 1
PROBLEM 1 (10 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.

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

(a) (2pts) If \(a = da'\) and \(b = db'\) where \(d = (a, b)\) then \((a', b') = 1\).

Answer: True.

We have \(d = ax + by\) for some \(x, y \in \mathbb{Z}\); thus \(d = da'x + db'y\) implies \(1 = a'x + b'y\), hence \((a', b') = 1\) because \((a', b')\) is the smallest positive integers that can be written as a integer linear combination of \(a'\) and \(b'\).

(b) (2pts) If \(c \neq 0\) and \(ca \equiv cb \pmod{m}\) then \(a \equiv b \pmod{m}\).

Answer: False.

For example, \(6 \cdot 2 \equiv 6 \cdot 1 \pmod{3}\) but \(2 \not\equiv 1 \pmod{3}\).

(c) (2pts) If \(a \equiv b \pmod{m}\) then \(c^a \equiv c^b \pmod{m}\).

Answer: False.

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

(d) (2pts) If \(1 \leq a \leq m - 1\) then \(a\) is invertible modulo \(m\).

Answer: False.

The integer \(a = 2\) is not invertible modulo \(m = 4\) and satisfies \(1 \leq 2 \leq 3 = m - 1\).

(e) (2pts) If \(0 \leq a, b \leq m - 1\) and \(a \equiv b \pmod{m}\) then \(a = b\).

Answer: True.

We have \(a - b = mk, k \in \mathbb{Z}\) and \(-(m - 1) \leq a - b \leq m - 1\). The unique multiple of \(m\) in this interval is zero, thus \(a - b = 0\), that is \(a = b\).
PROBLEM 2 (10 points)

(a) (2pts) State the definition of the inverse of an integer \(a\) modulo \(m\), where \(m\) is a positive integer.

Answer: Any integer \(x\) satisfying the congruence \(ax \equiv 1 \pmod{m}\) is called an inverse of \(a\) modulo \(m\).

(b) (8pts) Compute \(13^{-1} \pmod{55}\) using the Euclidean algorithm and back substitution.

Answer: Computing an inverse of 13 modulo 55 amounts to find the \(x\)-coordinate of a solution \((x, y)\) of the equation \(13x + 55y = 1\). We first use Euclidean algorithm to compute \((13, 55)\). Indeed,

\[
55 = 13 \cdot 4 + 3, \quad 13 = 3 \cdot 4 + 1, \quad 3 = 1 \cdot 3 + 0
\]
giving \((55, 13) = (13, 3) = (3, 1) = (1, 0) = 1\). We now apply back substitution

\[
1 = 13 - 3 \cdot 4 = 13 - (55 - 13 \cdot 4) \cdot 4 = 13 - 55 \cdot 4 + 13 \cdot 16 = 13 \cdot 17 + 55 \cdot (-4)
\]
to conclude that \((17, -4)\) is a solution of to the equation above. Thus \(x = 17 \pmod{55}\) is the inverse of 13 modulo 55.
PROBLEM 3 (10 points)

(a) (2pts) State the Chinese Reminder Theorem.

**Answer:** Let $m_1, m_2, \ldots, m_k \in \mathbb{Z}_{>0}$ and pairwise coprime. Let $b_1, b_2, \ldots, b_k \in \mathbb{Z}$. Then the system of congruences

\[
\begin{align*}
  x &\equiv b_1 \pmod{m_1} \\
  x &\equiv b_2 \pmod{m_2} \\
  &\vdots \\
  x &\equiv b_k \pmod{m_k}
\end{align*}
\]

has a unique solution modulo $m_1 \cdot m_2 \cdot \ldots \cdot m_k$.

(b) (8pts) Compute $13^{-1} \pmod{55}$ using the Chinese reminder theorem.

**Answer:** We want to find an integer $x$ satisfying the congruence $13x \equiv 1 \pmod{55}$. Since $55 = 5 \cdot 11$ such integer $x$ will also satisfy the congruences

\[
3x \equiv 1 \pmod{5} \quad \text{and} \quad 2x \equiv 1 \pmod{11}.
\]

Note that 2 is the inverse of 3 mod 5 and 6 is the inverse of 2 mod 11. Then, the previous congruences are equivalent to

\[
x \equiv 2 \pmod{5} \quad \text{and} \quad x \equiv 6 \pmod{11}.
\]

We now compute the solution. Let $M = 5 \cdot 11 = 55$, $M_1 = 11$ and $M_2 = 5$. The congruences

\[
11x \equiv 1 \pmod{55} \quad \text{and} \quad 5x \equiv 1 \pmod{55}
\]

have solutions $y_1 = 1$ and $y_2 = 9$, respectively. We conclude that the unique solution modulo $M$ is

\[
x \equiv 2 \cdot 11 \cdot 1 + 6 \cdot 5 \cdot 9 \equiv 22 + 270 \equiv 22 + 50 \equiv 77 \equiv 17 \pmod{55}
\]
PROBLEM 4 (15 points)

(a) (8pts) Show that $7^{100} \equiv 1 \pmod{1000}$.

Answer: Note that $1000 = 2^3 \cdot 5^3 = 8 \cdot 125$. By the CRT it suffices to show that

$$7^{100} \equiv 1 \pmod{8} \quad \text{and} \quad 7^{100} \equiv 1 \pmod{125}. $$

Since $\phi(8) = 4$ and $\phi(5^3) = 4 \cdot 5^2 = 100$ we have from Euler’s theorem that

$$(7^4)^{25} \equiv 1^{25} \equiv 1 \pmod{8} \quad \text{and} \quad 7^{100} \equiv 1 \pmod{125},$$

as desired.

(b) (7pts) Find the three last decimal digits of $7^{999}$.

(Hint: $1001 = 7 \cdot 11 \cdot 13$)

Answer: Note that $7 \cdot 7^{999} = 7^{1000} \equiv (7^{100})^{10} \equiv 1 \pmod{1000}$, where we used (a) in the last congruence. Thus $7^{999} \equiv 7^{-1} \pmod{1000}$. Now $1001 = 7 \cdot 11 \cdot 13$ implies $7 \cdot (11 \cdot 13) \equiv 1 \pmod{1000}$ that is $7^{-1} \equiv 11 \cdot 13 = 143 \pmod{1000}$. We conclude that $7^{999} \equiv 143 \pmod{1000}$ then 143 are the three last decimal digits of $7^{999}$. 
PROBLEM 5 (15 points)

(a) (2pts) Explain what it means for an integer $n > 0$ to be a pseudoprime to the base $b \in \mathbb{Z}_{\geq 2}$.

**Answer:** An integer $n > 0$ is a pseudoprime to base $b \in \mathbb{Z}_{\geq 2}$ if it fools Fermat’s test in base $b$. That is, if $n$ is composite and satisfies $b^{n-1} \equiv 1 \pmod{n}$.

(b) (9pts) Prove that $1729 = 7 \cdot 13 \cdot 19$ is a Carmichael number.

**Answer:** A composite integer $n$ is a Carmichael number if $b^{n-1} \equiv 1 \pmod{n}$ for all bases $b$ such that $(n,b) = 1$.

Let $n = 1729$ and $b \in \mathbb{Z}$ satisfy $(b,n) = 1$. Then $(b,7) = (b,13) = (b,19) = 1$ and by Fermat’s Little Theorem we have

$$b^6 \equiv 1 \pmod{7}, \quad b^{12} \equiv 1 \pmod{13}, \quad b^{18} \equiv 1 \pmod{19}.$$

Note that $n - 1 = 1728$ is divisible by 4 (the last 2 digits are 28 which is divisible by 4) and by 9 (the sum of its digits is 18), hence $n - 1$ is also divisible by 6, 12 and 18. We conclude that

$$b^{n-1} \equiv 1 \pmod{7}, \quad b^{n-1} \equiv 1 \pmod{13}, \quad b^{n-1} \equiv 1 \pmod{19}$$

and by CRT it follows that

$$b^{n-1} \equiv 1 \pmod{n},$$

as desired.

(c) (4pts) Show, without using the explicit factorization of 1729, but using the following congruences instead, that 1729 is composite

$$2^{18} \equiv 1065 \pmod{1729} \quad \text{and} \quad 2^{36} \equiv 1 \pmod{1729}.$$

**Answer:** Let $x = 2^{18}$. We have $x^2 = 2^{36} \equiv 1 \pmod{1729}$, hence if 1729 is a prime we also have $x \equiv \pm 1 \pmod{1729}$. This means $x = 2^{18} \equiv 1065 \equiv \pm 1 \pmod{1729}$ which is impossible. We conclude that 1729 is composite.
An old receipt has faded. It reads “88 chickens cost a total of \$x4.2y”, where \(x\) and \(y\) are unreadable digits. How much did the 88 chickens cost?

**Answer:** We know that the total cost being \(x42y\) cents is divisible by 88 = 8 \cdot 11 and so is divisible by both 11 and \(2^3 = 8\).

Thus \(42y\) is divisible by \(2^3 = 8\), and \(2y\) is divisible by \(2^2 = 4\) and \(y\) is divisible by 2. The only number \(0 \leq y < 10\) satisfying this is \(y = 4\).

As \(x424\) is divisible by 11 we require that

\[ x - 4 + 2 - 4 = x - 6 \]

is divisible by 11. The only number \(0 \leq x < 10\) satisfying this is \(x = 6\). Thus the total cost was \$64.24.
PROBLEM 7 (20 points)

Show there is no positive integer $n$ such that $\phi(n) = 14$, where $\phi$ is the Euler $\phi$-function.

**Answer:** Suppose $\phi(n) = 14$. 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

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

From the formula it follows that $p - 1 \mid 14$ for each prime $p \mid n$. That is $p - 1 \in \{1, 2, 7, 14\}$ implying $p = 2$ or $3$. Hence $n$ has the form $n = 2^a3^b$ where $a, b \geq 0$ are not both 0. From the formula we see that if $a > 0$ or $b > 0$ we have respectively

$$\phi(2^a) = 2^{a-1} \quad \text{or} \quad \phi(3^b) = 3^{b-1} \cdot 2.$$

Finally, since $\phi(n) = \phi(2^a)\phi(3^b)$ the previous equalities show that 7 does not divide $\phi(n)$. We conclude there is no integer $n$ satisfying $\phi(n) = 14$. 