Your Name: ______________________________
For purpose of anonymous grading, please do not write your name on the subsequent pages.

This examination consists of 6 problems, which are subdivided into 9 questions, where each question counts for the explicitly given number of points, adding to a total of 46 points. Please write your answers in the spaces indicated, or below the questions, using the back of the sheets for completing the answers and for all scratch work, if necessary. You are allowed to consult two 8.5in × 11in sheets with notes, but not your book or your class notes. If you get stuck on a problem, it may be advisable to go to another problem and come back to that one later.

You will have 75 minutes to do this test.

Good luck!

Problem 1 _____

2 _____

3 _____

4 _____

5 _____

6 _____

Total _____
Problem 1 (16 points)

(a, 4pts) Let $p$ be a prime number $\geq 19$ with $p \equiv 4 \pmod{5}$.
   (i) please prove that $3(p - 1) + 1 = 3p - 2$ is divisible by 5.
   (ii) please prove that for all $a \in \mathbb{Z}_p$ we have for $b = a^{(3p-2)/5} \mod p$ that $b^5 \equiv a \pmod{p}$.

(b, 4pts) The integer 341 is a pseudo-prime (to base 2) but **not** a Carmichael number. Please explain what both mean.

(c, 4pts) Please show that $3^{100} \equiv 1 \pmod{1000}$. [Hint: factor the modulus $1000 = 8 \cdot 125$.]

(d, 4pts) Please compute residues $x, y \in \mathbb{Z}_8$, or prove that none exist, such that

\[
\begin{align*}
x + 3y & \equiv 5 \pmod{8} \\
5x + y & \equiv 6 \pmod{8}.
\end{align*}
\]
Problem 2 (6 points): Please prove that there are infinitely many composite integers that are \( \equiv 5 \pmod{6} \).

Problem 3 (6 points): By completing the \( 3 \cdot 10 \) entries in the following table in terms of prime numbers \( p \) and \( q \) with \( p \neq q \), please verify Gauss’s Theorem for Euler’s \( \phi \) function and its associate Möbius inversion formula for \( n = p^2q^2 \):

<table>
<thead>
<tr>
<th></th>
<th>( d )</th>
<th>( \phi(d) )</th>
<th>( \mu(d) )</th>
<th>( \mu(d) \cdot \frac{n}{d} )</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>2.</td>
<td>( p )</td>
<td>( p-1 )</td>
<td>1</td>
<td>( p-1 )</td>
</tr>
<tr>
<td>3.</td>
<td>( p^2 )</td>
<td>( p^2-1 )</td>
<td>1</td>
<td>( p^2-1 )</td>
</tr>
<tr>
<td>4.</td>
<td>( q )</td>
<td>( q-1 )</td>
<td>1</td>
<td>( q-1 )</td>
</tr>
<tr>
<td>5.</td>
<td>( pq )</td>
<td>( \phi(p)\phi(q) )</td>
<td>( \mu(p)\mu(q) )</td>
<td>( \mu(p)\mu(q) \frac{n}{d} )</td>
</tr>
<tr>
<td>6.</td>
<td>( p^2q )</td>
<td>( p^2q-1 )</td>
<td>( \mu(p)\mu(q) )</td>
<td>( \mu(p)\mu(q) \frac{n}{d} )</td>
</tr>
<tr>
<td>7.</td>
<td>( q^2 )</td>
<td>( q^2-1 )</td>
<td>1</td>
<td>( q^2-1 )</td>
</tr>
<tr>
<td>8.</td>
<td>( pq^2 )</td>
<td>( \phi(p)\phi(q^2) )</td>
<td>( \mu(p)\mu(q^2) )</td>
<td>( \mu(p)\mu(q^2) \frac{n}{d} )</td>
</tr>
<tr>
<td>9.</td>
<td>( p^2q^2 )</td>
<td>( p^2q^2-1 )</td>
<td>( \mu(p^2)\mu(q^2) )</td>
<td>( \mu(p^2)\mu(q^2) \frac{n}{d} )</td>
</tr>
<tr>
<td>10.</td>
<td>( \sum_{d \text{ divides } p^2q^2 \text{ and } d \geq 1} )</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

\( n = p^2q^2 \)
Problem 4 (8 points): Consider $2310 = 5 \cdot 6 \cdot 7 \cdot 11$ and let $a \in \mathbb{Z}_{2310}$ with

$$
a \equiv 4 \pmod{5},
\quad a \equiv 5 \pmod{6},
\quad a \equiv 4 \pmod{7},
\quad a \equiv 7 \pmod{11}.
$$

Please compute $y_0 \in \mathbb{Z}_5, y_1 \in \mathbb{Z}_6, y_2 \in \mathbb{Z}_7$ and $y_3 \in \mathbb{Z}_{11}$ such that

$$a = y_0 + y_1 \cdot 5 + y_2 \cdot 5 \cdot 6 + y_3 \cdot 5 \cdot 6 \cdot 7.$$

Then compute $a$. Please show all your work.
Problem 5 (5 points): Let \( k = 2^4 + 2^2 + 2 + 1 = 23 \). Please show how one can compute \( a^k \mod n \) with 7 multiplications of residues modulo \( n \).

Problem 6 (5 points): Please consider the following (toy) instance of the RSA: the public modulus is \( n = 77 \) and the public (enciphering) exponent is \( k = 43 \). Please compute the private deciphering exponent \( j \) such that \( (M^{43})^j \equiv M \mod 77 \) (at least for all \( M \in U_{77} \)). Please show your work.