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

This examination consists of 5 problems, which are subdivided into 9 questions, where each question counts for the explicitly given number of points, adding to a total of 44 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 60 minutes to do this test.

Good luck!

Problem 1 ______
2 ______
3 ______
4 ______
5 ______

Total ______
Problem 1 (16 points)

(a, 4pts) True or false:
\[ \forall m \in \mathbb{Z}_{\geq 2}, a, b, c \in \mathbb{Z}_m: c \neq 0 \text{ and } ac \equiv bc \pmod{m} \implies a \equiv b \pmod{m}. \]
Please explain.

(b, 4pts) Please compute all solutions \(x \in \mathbb{Z}_{11}\) for
\[ 7 \cdot x^2 \equiv 10 \pmod{11}. \]
Please show your work.

(c, 4pts) Please compute \(3^{2^{10}} \mod 10\). [Hint: use Euler’s theorem.]

(d, 4pts) True or false: \(1729 = 7 \cdot 13 \cdot 19\) is a Carmichael number. Please explain.
Problem 2 (6 points): For which integers $n \geq 0$ is $7^{2n+1} - 6^{n+1}$ divisible by 43? Please justify your answer.

Problem 3 (6 points): Please make a table of all positive divisors $d$ of $140 = 2^2 \cdot 5 \cdot 7$ and the corresponding $\phi(d)$ values. Also, please verify Gauss’s theorem: $140 = \sum_{d>0 \text{ and } d|140} \phi(d)$. 
**Problem 4** (8 points): Consider $360 = 5 \cdot 8 \cdot 9$ and let $a \in \mathbb{Z}_{360}$ with

\[
\begin{align*}
    a &\equiv 4 \pmod{5}, \\
    a &\equiv 2 \pmod{8}, \\
    a &\equiv 8 \pmod{9}.
\end{align*}
\]

Please compute $y_0 \in \mathbb{Z}_5, y_1 \in \mathbb{Z}_8$ and $y_2 \in \mathbb{Z}_9$ such that

\[
a = y_0 + y_1 \cdot 5 + y_2 \cdot 5 \cdot 8.
\]

Please show all your work.
Problem 5 (8 points): Consider the following instance of the RSA:
the public modulus is \( n = 3 \cdot 11 = 33 \) and the public (enciphering) exponent is \( e = 7 \).

(a, 4pts) Please compute the private deciphering exponent \( j \) such that \((M^e)^j \equiv M \pmod{n}\) (at least for all \( M \in \mathbb{Z}_n \) that are relatively prime to \( n \)).

(b, 4pts) Please encrypt the message \( M_1 = (2 \mod 33) \). Then decrypt the produced cypher number in \( \mathbb{Z}_n \). Also try to encrypt \( M_2 = (3 \mod 33) \) and then decrypt the produced cypher number; note that 3 is not relatively prime to \( n \). Please show all your work.