Problem 1

2 _____
3 _____
4 _____
5 _____
6 _____

Total _____

If you are taking the exam later, please sign the following statement:

_I, ____________________, affirm that I have no knowledge of the contents of this exam._

__________________________
Signature
Problem 1 (16 points)

(a, 4pts) True or false: \( \forall a \in \mathbb{Z}_{16}, a \) an odd integer: \( a^4 \equiv 1 \pmod{16} \).

(b, 4pts) True or false: \( 63973 = 7 \cdot 13 \cdot 19 \cdot 37 \) is a Carmichael number. Please explain.

(c, 4pts) Please compute \( 2^{100} \mod{100} \), showing your work. Hint: \( 100 = 4 \cdot 25 \), use Euler’s theorem modulo 25.

(d, 4pts) Please show how to compute \( a^{23} \mod{n} \) for \( a \in \mathbb{Z}_n \) with 6 multiplications modulo \( n \).
Problem 2 (6 points): Please prove for all prime numbers $p \geq 2$ and for all integers $k$ with $1 \leq k \leq p - 1$ that the binomial coefficient $\binom{p}{k}$ satisfies $\binom{p}{k} \equiv 0 \pmod{p}$.

Problem 3 (6 points): Please determine two integers $n_1 \geq 1, n_2 \geq 1, n_1 \neq n_2$ such that $\phi(n_1) = \phi(n_2) = 20$, where $\phi$ is Euler’s phi-function.
Problem 4 (8 points): Consider $2015 = 31 \cdot 13 \cdot 5$ and let $a \in \mathbb{Z}_{2015}$ with

\[
\begin{align*}
    a &\equiv 18 \pmod{31}, \\
    a &\equiv 1 \pmod{13}, \\
    a &\equiv 4 \pmod{5}.
\end{align*}
\]

Please compute $y_0 \in \mathbb{Z}_{31}$, $y_1 \in \mathbb{Z}_{13}$ and $y_2 \in \mathbb{Z}_{5}$ such that

\[a = y_0 + y_1 \cdot 31 + y_2 \cdot 31 \cdot 13.\]

Then compute $a$. Please show all your work.
Problem 5 (5 points): The Miller-Rabin algorithm is a randomized algorithm of the Monte Carlo kind for the establishing the primality of an integer input. Please explain what that means.

Problem 6 (5 points): Please consider the following (toy) instance of the RSA: the public modulus is $n = 55$ and the public (enciphering) exponent is $k = 27$. Please compute the private deciphering exponent $j$ such that $\left(M^{27}\right)^j \equiv M \pmod{55}$ (at least for all $M \in U_{55}$). With the computed $j$, please decipher the message $M$ from the cipher text $C = \left(M^{27} \mod 55\right) = 49$. Please show your work.