Problem 1 (16 points)

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

**True**

\[ a^4 - 1 = (a+1)(a-1)(a^2+1) \]

\( a+1, a-1 \) are both even, and one of the two is div. by 4, so the product is div. by 4.

\( a^2+1 \) is even, so the product is div. by 4.

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

\[ \begin{align*}
37 - 1 &= 36 \\
19 - 1 &= 18 \\
13 - 1 &= 12 \\
7 - 1 &= 6
\end{align*} \]

36 \mid 63973 - 1

then by Korselt's Criterion, 63973 is a C.N.

36 = 2^2 \cdot 9

9 \mid 6 + 3 + 9 + 7 + 2

4 \mid 72

True

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

\[ \begin{align*}
\phi(25) &= 20 \\
(2^{20})^5 &= 2^{100} \equiv 1 \pmod{25} \\
2^{100} &\equiv 0 \pmod{4}
\end{align*} \]

\[ a = 2^{100} \equiv 0 \pmod{4} \]

1 + x \cdot 25 \equiv 0 \pmod{4}

(d, 4pts) Please show how to compute \( a^{23} \pmod{n} \) for \( a \in \mathbb{Z}_n \) with 6 multiplications modulo \( n \).

1. \( a \cdot a = a^2 = b \)
2. \( a \cdot b = a^3 = c \)
3. \( b \cdot c = a^5 = d \)
4. \( a \cdot d = a^{10} = e \)
5. \( e \cdot e = a^{20} = f \)
6. \( f \cdot c = a^{23} \)
**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 \( \binom{p}{k} \equiv 0 \pmod{p} \).

\[
\binom{p}{k} = \frac{p!}{(p-k)!k!} = \frac{p(p-1)\ldots(p-k+1)}{1\cdot2\cdot\ldots\cdot k} \in \mathbb{Z}
\]

Since \( 1 \leq k \leq p - 1 \) we have \( \frac{(p-1)\ldots(p-k+1)}{1\cdot2\cdot\ldots\cdot k} = 1 \in \mathbb{Z} \)

\[
\Rightarrow \binom{p}{k} = p \cdot l \equiv 0 \pmod{p} \Rightarrow \binom{p}{k} \equiv 0 \pmod{p}
\]

**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.

\[
\phi(n) = n \cdot \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \ldots = \phi(n_1) \cdot \phi(n_2) = 20 = 4 \cdot 5 = 2 \cdot 10
\]

\[
\phi(25) = 25 \left(1 - \frac{1}{5}\right) = 20 \quad \text{(from Problem 1c)}
\]

\[
\phi(50) = 50 \left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{5}\right) = 20
\]

\[
\phi(44) = 44 \left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{11}\right) = 20 = \phi(4) \cdot \phi(11)
\]

\[
\phi(33) = \phi(3) \cdot 3 \phi(11) = 2 \cdot 10 = 20
\]

\[
\phi(66) = \phi(6) \cdot \phi(11) = 2 \cdot 10 = 20
\]
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.

\[
\begin{align*}
    y_0 &= 18, \\
    18 + y_1 \cdot 31 &\equiv 1 \pmod{13}, \\
    5 + y_1 \cdot 5 &\equiv 1 \pmod{13}, \\
    y_1 \cdot 5 &\equiv 9 \pmod{13}, \\
    y_1 &\equiv 7 \pmod{13}, \\
    y_1 &= 7.
\end{align*}
\]

\[
\begin{align*}
    18 + 7 \cdot 31 + y_2 \cdot 31 \cdot 13 &\equiv 4 \pmod{5}, \\
    3 + 2 + y_2 \cdot 3 &\equiv 4 \pmod{5}, \\
    y_2 \cdot 3 &\equiv 4 \pmod{5}, \\
    y_2 &\equiv 3 \pmod{5}, \\
    y_2 &= 3.
\end{align*}
\]

\[a = 18 + 7 \cdot 31 + 3 \cdot 31 \cdot 13 = 1444.\]
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.

The algorithm uses randomization to achieve speed, but this is at the expense of always being correct. Simply put, the algorithm is always fast and probably correct.

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 \( (M^{27})^j \equiv M \pmod{55} \) (at least for all \( M \in U_{55} \)). With the computed \( j \), please decipher the message \( M \) from the cipher text \( C = (M^{27} \mod 55) = 49 \). Please show your work.

\[
\begin{array}{c|c|c|c}
\text{r} & \text{q} & \text{d} \\
1 & 40 & 1 & 0 \\
1 & 27 & 0 & 1 \\
1 & 13 & 1 & -1 \\
2 & 1 & -2 & 3 \\
\end{array}
\]

\( q = 3 \)

\( M = (49)^3 \mod 55 \)

\( = (-6)(-6)(-6_5) = 36(-2)^3 \)

\( = (-19)3.2 = 57.2 \)

\( = 2.2 = 4 \pmod{55} \)