Problem 1 (16 points)

(a, 4pts) Let \( p = 5, 19, 47, 61, \ldots \) be a prime number with \( p \equiv 5 \pmod{7} \).

(i) please prove that \( 5p - 4 \) is divisible by 7.

(ii) please prove that for all \( a \in \mathbb{Z}_p \) we have for \( b = a^{(5p-4)/7} \pmod{p} \) that \( b^7 \equiv a \pmod{p} \).

\[
(i) \quad 5p - 4 \equiv 5 \cdot 5 - 4 \equiv 21 \equiv 0 \pmod{7} \\
(ii) \quad b^7 \equiv (a^{(5p-4)/7})^7 \equiv a^{5p-4} \equiv a \cdot a^{5p-5} \\
= a \cdot (a^p)^5 \equiv a \cdot 1^5 \equiv a \pmod{p}
\]

(b, 4pts) Please compute the number of residues \( a \in \mathbb{Z}_{63973} \) that satisfy \( a^{63972} \equiv 1 \pmod{63973} \).

[Hint: 63973 = 7 \cdot 13 \cdot 19 \cdot 37; prove first that 63973 is a Carmichael number.]

\[
63972 = 2^2 \cdot 3^2 \cdot 17 \cdot 777 = 36 \cdot 1777 \\
\text{and } 7 - 1 = 6, 13 - 1 = 12, 19 - 1 = 18, 37 - 1 = 36 \\
\text{all divide } 36 \\
\phi(63973) = 6 \cdot 12 \cdot 18 \cdot 36 = 46656 \text{ residues } a
\]

(c, 4pts) Please compute \( 2^{102} \pmod{1000} \), showing all your work.

\[
1000 = 8 \cdot 125 \quad 2^{102} \equiv 0 \pmod{8} \\
\phi(125) = 100 \quad 2^{100} \equiv 1 \pmod{125} \Rightarrow 2^{102} \equiv 4 \pmod{125} \\
a = 4 + y \cdot 125 \equiv 0 \pmod{8} \\n5^{-1} \equiv 5 \pmod{8} \\
a \equiv 4 \cdot 5 \equiv 4 \pmod{8} \quad \Rightarrow a = 504
\]

(d, 4pts) Please show how to compute \( a^{31} \pmod{n} \) for \( a \in \mathbb{Z}_n \) with 7 multiplications modulo \( n \).

\[
a^2, \quad a^3 = a \cdot a^2, \quad a^5 = a^2 \cdot a^3, \quad a^{10} = a^5 \cdot a^5 \\
\]

\[
a^{15} = a^5 \cdot a^{10}, \quad a^{30} = a^{15} \cdot a^{15}, \quad a^{31} = a \cdot a^{30}
\]

\[
\]

\[
\]

\[
\]

\[
\]

\[
\]

\[
\]

\[
\]
Problem 2 (7 points): Please prove for all odd integers $a$ and all integers $n$ with $n \geq 1$ that $a^{2^n} \equiv 1 \pmod{2^{n+2}}$. [Hint: use mathematical induction on $n$.]

\[ n = 1: \quad a^2 = (2b+1)^2 = 4b^2 + 4b + 1 = 4b(b+1) + 1 \equiv 1 \pmod{8} \]

\[ a^{2^n+1} - 1 = (a^{2^n} + 1)(a^{2^n} - 1) = 2^{n+1} \cdot L \cdot M \text{ \text{\text{Hypothesis}} \text{ \text{\text{Hypothesis}}}} \]

\[ 2 \cdot L \cdot 2^{n+2} \cdot M \equiv 0 \pmod{2^{n+3}} \]

because

\[ a^{2^n} + 1 \equiv 1^2 + 1 = 0 \pmod{2} \]

Problem 3 (6 points): By completing the 3·9 entries in the following table in terms of prime numbers $p, q, r$ with $2 \leq p < q < r$, please verify Gauss’s Theorem for Euler’s $\phi$ function and its associate Möbius inversion formula for $n = pqr$:

<table>
<thead>
<tr>
<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>$pq$</td>
</tr>
<tr>
<td>2.</td>
<td>$p$</td>
<td>$p-1$</td>
<td>$-1$</td>
</tr>
<tr>
<td>3.</td>
<td>$q$</td>
<td>$q-1$</td>
<td>$-1$</td>
</tr>
<tr>
<td>4.</td>
<td>$r$</td>
<td>$r-1$</td>
<td>$-1$</td>
</tr>
<tr>
<td>5.</td>
<td>$pq$</td>
<td>$(p-1)(q-1)$</td>
<td>1</td>
</tr>
<tr>
<td>6.</td>
<td>$pr$</td>
<td>$(p-1)(r-1)$</td>
<td>1</td>
</tr>
<tr>
<td>7.</td>
<td>$qr$</td>
<td>$(q-1)(r-1)$</td>
<td>1</td>
</tr>
<tr>
<td>8.</td>
<td>$pqr$</td>
<td>$(p-1)(q-1)(r-1)$</td>
<td>-1</td>
</tr>
<tr>
<td>9.</td>
<td>$\sum$</td>
<td>$pq$</td>
<td>0</td>
</tr>
</tbody>
</table>

\[ d \text{ divides } pqr \text{ and } d \geq 1 \]
Problem 4 (8 points): Consider $4042 = 43 \cdot 47 \cdot 2$ and let $a \in \mathbb{Z}_{4042}$ with

$$a \equiv 1 \pmod{43}, \quad a \equiv 5 \pmod{47}, \quad a \equiv 0 \pmod{2}.$$ 

Please compute $y_0 \in \mathbb{Z}_{43}, y_1 \in \mathbb{Z}_{47}$ and $y_2 \in \mathbb{Z}_2$ such that

$$a = y_0 + y_1 \cdot 43 + y_2 \cdot 43 \cdot 47.$$ 

Then compute $a$. Please show all your work.

\[
y_0 = 1 \quad \quad a = 1 + y_1 \cdot 43 \equiv 5 \pmod{47}
\]

\[
\begin{array}{ccc}
47 & 1 & 0 \\
43 & 0 & 1 \\
1 & 4 & 1 \quad -1 \\
10 & 3 & -10 \quad 11 \\
1 & 1 & 11 \quad -12
\end{array}
\]

\[
y_1 = (5 - 1) \cdot (-12) \equiv 46 \pmod{47} \equiv 43^{-1} \pmod{47}
\]

\[
1 + 46 \cdot 43 + y_2 \cdot 43 \cdot 47 \equiv 0 \pmod{2}
\]

\[
y_2 \equiv 0 - 1 \equiv 1 \pmod{2}
\]

\[
a = 1 + 46 \cdot 43 + 43 \cdot 47 = 4000
\]

Check: $4000 \mod 43 = 1$

\[
4000 \mod 47 = 5
\]
Problem 5 (5 points): Please consider the following (toy) scenario of the RSA: Bob discovers an old ciphertext $C = 48$ from Alice, and his public exponent $k = 29$ and private factorization of the modulus $n = 95 = 5 \cdot 19$. Please explain how Bob would recover Alice’s (clear text) message $M$ and what $M$ actually is for the given $C = 48$. Please show your work.

$$\Phi(95) = 4 \cdot 18 = 72$$

$$\begin{bmatrix}
72 & 1 & 0 \\
29 & 0 & 1 \\
2 & 1 & -2 \\
2 & 1 & -2 & 5
\end{bmatrix}$$

$M = C^5 \mod n = 48^5 \mod 95$

$= 3$

Check: $3^{29} \mod 95 = 48$

Problem 6 (6 points): Please consider the function $M(n) = \sum_{d \mid n, d \geq 1} \mu(d)$.

(a) Please prove that $M(1) = 1$ and $M(n) = 0$ for $n \geq 2$. (Cf. Problem 3, \(\mu(d)\)-column.)

(b) Please verify the Möbius Inversion Formula for $F = M$ and $f = \mu$:

$$\mu(n) = \sum_{d \mid n, d \geq 1} \mu(d) M\left(\frac{n}{d}\right).$$

(a) $\mu(n)$ is number-theoretic $\Rightarrow M(n)$ is number-theoretic. Therefore

$M(p^e_1 \cdots p^e_t) = M(p^e_1) \cdots M(p^e_t)$

and

$M(p^e) = \mu(1) + \mu(p) + \mu(p^2) + \cdots + \mu(p^e) = 1 - 1 + 0 + \cdots + 0 = 0$

(b) $\sum_{d \mid n, d \geq 1} \mu(d) M\left(\frac{n}{d}\right) = \mu(n) \cdot M(1) + 0 + \cdots + 0 = \mu(n).$