(1) Find a primitive root mod 71. (20 points)

(2) Let \( n_1, n_2, \ldots, n_k \geq 1 \) be integers. Using the criterion we proved in class, show that the direct product of cyclic groups
\[
\mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \times \cdots \times \mathbb{Z}/n_k\mathbb{Z}
\]
is cyclic if and only if \( n_1, n_2, \ldots, n_k \) are coprime in pairs. (20 points)

(3) (a) Show that for \( k \geq 2 \), \( 5^{2^{k-2}} \equiv 1 + 2^k \mod 2^{k+1} \).
(b) Show that for \( k \geq 2 \),
\[
(\mathbb{Z}/2^k\mathbb{Z})^\times \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{k-2}\mathbb{Z},
\]
where the generators are \(-1\) and 5. More precisely, the homomorphism from \( \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{k-2}\mathbb{Z} \) to \( (\mathbb{Z}/2^k\mathbb{Z})^\times \) that sends \((\bar{1}, \bar{0})\) to \(-1\) and \((\bar{0}, \bar{1})\) to 5 is an isomorphism.

Be careful: One group is written additively, the other multiplicatively! (10+10 points)

(4) Let \( n > 0 \). Show that \( (\mathbb{Z}/n\mathbb{Z})^\times \) is cyclic if and only if \( n = 1, 2, 4, p^e \), or \( 2p^e \) with \( p \) an odd prime (and \( e \geq 1 \)).

HINTS. (a) Use the Chinese Remainder Theorem.
(b) Use the results of the preceding two problems. (20 points)

(5) (a) Show that the number \( 2^m + 1 \) (for \( m \geq 1 \)) can be prime only when \( m = 2^n \) is a power of 2.
(b) Show that a prime number \( p \) dividing \( 2^{2^n} + 1 \) must satisfy \( p \equiv 1 \mod 2^{n+1} \).

HINT. What is the order of \( \bar{2} \) in \( \mathbb{F}_p^\times \)? (8+12 points)

(6) **Bonus Problem**

A composite integer \( n > 1 \) that “pretends” to be prime in the sense that
\[
a^{n-1} \equiv 1 \mod n \quad \text{for all } a \perp n
\]
is called a **Carmichael Number**.

(a) Show that a Carmichael Number must be odd and squarefree and must have at least three prime factors.

(b) Find the smallest Carmichael Number. (15+10 points)