Problems:

1. (a) Let \( r \) be a positive integer, and let \( p \) be prime with \( \gcd(r, p - 1) = 1 \). Thus \( r \) has an inverse modulo \( p - 1 \). Let \( s \) denote the inverse,
\[
s = r^{-1} \mod p - 1.
\]
Show that for every \( a \) modulo \( p \), the value
\[
a^s \mod p
\]
is an \( r \)th root of \( a \) modulo \( p \).

(b) Let \( q \) be prime, and let \( p \) be prime with \( q \mid p - 1 \) but \( q^2 \nmid p - 1 \). Thus \( q \) has an inverse modulo \( (p - 1)/q \). Let
\[
s = q^{-1} \mod (p - 1)/q.
\]
Suppose that \( a \) is a \( q \)th power modulo \( p \). Show that the value
\[
a^s \mod p
\]
is a \( q \)th root of \( a \) modulo \( p \).

2. (a) Let \( p \) be prime and let \( n > 1 \). Show that the polynomial
\[
f(X) = X^n - pX + p
\]
has no rational root.

(b) Let \( p \) be prime, and let \( c \) be an integer not divisible by \( p \). Show that the polynomial
\[
g(X) = X^p - X + c
\]
has no rational root.

3. Use fast modular exponentiation to compute
\[
72^{50} \mod 101.
\]
What does the result say about a square root of \(-1\) modulo \( 101 \)?

4. Explain why for any positive integer \( n \),
\[
\sum_{d|n} \varphi(d) = n.
\]

5. (a) Supply the two missing calculations in the handout’s proof of the Sun-Ze Theorem.

(b) Use the map \( g \) in the handout’s proof of the Sun-Ze Theorem to find an equivalence class \( c \mod 77 \) such that
\[
c = 3 \mod 7, \quad c = 7 \mod 11.
\]
Use the map $g$ in the handout’s proof of the Sun-Ze Theorem to find an equivalence class $c \mod 1001$ such that
\[ c = 3 \mod 7, \quad c = 7 \mod 11, \quad c = 4 \mod 13. \]