Problem 1 (15pts) Give all primitive roots of 19. You do not need to simplify or reduce your answers modulo 19.

Solution. Note that \( \phi(19) = 18 \), so we know that the order of any element is a divisor of 18, that is, 1, 2, 3, 6, 9, or 18. Let us consider the order of 2.

\[
\begin{align*}
2^1 &\equiv 2 \not\equiv 1 \pmod{19} \\
2^2 &\equiv 4 \not\equiv 1 \pmod{19} \\
2^3 &\equiv 8 \not\equiv 1 \pmod{19} \\
2^6 &\equiv 2^{42} \equiv 16 \cdot 2^2 \equiv -3 \cdot 4 \equiv -12 \equiv 7 \not\equiv 1 \pmod{19} \\
2^9 &\equiv 2^6 \cdot 2^2 \equiv 7 \cdot 4 \cdot 2 \equiv 14 \cdot 4 \equiv -5 \cdot 4 \equiv -20 \equiv -1 \not\equiv 1 \pmod{19} \\
2^{18} &\equiv 1 \pmod{19}
\end{align*}
\]

So the order of 2 is 18. Since the order of 2 \( h = 18 \) \((h, 18)\), it follows that the order 18 elements are \( 2, 2^5, 2^7, 2^{11}, 2^{13}, \) and \( 2^{17} \) because 1, 5, 7, 11, 13, and 17 are the possible exponents less than or equal to 18 which are relatively prime to 18. Note that we know that we got them all because by a theorem there are \( \phi(\phi(19)) = \phi(18) = 6 \) primitive roots. \( \square \)

Problem 2 (10pts) Prove that \( 31 \mid 4(29)! + 5! \).

Solution. By Wilson’s theorem we know that \( (30)! \equiv -1 \pmod{31} \), and thus \( -1 \equiv (30)! \equiv 30(29)! \equiv (30 - 31)(29)! \equiv (-1)(29)! \pmod{31} \), or \( (29)! \equiv 1 \pmod{31} \).

We also have \( 5! = 5 \cdot 4 \cdot 3 \cdot 2 = (5 \cdot 3 \cdot 2) \cdot 4 \equiv 30 \cdot 4 \equiv -1 \cdot 4 \equiv -4 \pmod{31} \).

So \( 4(29)! + 5! \equiv 4(1) + (-4) \equiv 0 \pmod{31} \), and thus \( 31 \mid 4(29)! + 5! \). \( \square \)

Problem 3 (10pts) Prove that \( f(n) = \sum_{d \mid n} \frac{\tau(d)}{\sigma(d)} \) is a multiplicative number theoretic function.

Solution. Since \( \sigma(n) \neq 0 \) for all \( n \in \mathbb{N}_{>0} \) (given \( n \), there are always relatively prime numbers smaller than it, for instance, \( 1 \leq n \) and \( (1, n) = 1 \), so that \( \sigma(n) \geq 1 \)), this function is certainly number theoretic. Furthermore, we have a theorem which states that \( F(n) = \sum_{d \mid n} f(d) \) is multiplicative if \( f(n) \) is multiplicative. Thus it is enough to show that \( \frac{\tau(n)}{\sigma(n)} \) is multiplicative. Of course, we know that both \( \sigma \) and \( \tau \) are multiplicative. So let \( n, m \in \mathbb{N}_{>0} \) such that \( (m, n) = 1 \). We have \( \frac{\tau(nm)}{\sigma(nm)} = \frac{\tau(n)\tau(m)}{\sigma(n)\sigma(m)} = \frac{\tau(n)}{\sigma(n)} \frac{\tau(m)}{\sigma(m)} \) as required. \( \square \)
Problem 4 (15pts) Suppose that \( n = 2^p \) where \( p \) is an odd prime. Prove that \( a^{n-1} \equiv a \pmod{n} \) for any integer \( a \).

Solution. Since \( (2, p) = 1 \), it is enough to demonstrate that \( 2 | a^{n-1} - a \) and \( p | a^{n-1} - a \). If \( (a, 2) \neq 1 \), then \( 2 | a \), and thus \( a \equiv 0 \pmod{2} \), whence \( a^{n-1} \equiv a \pmod{2} \) and \( 2 | a^{n-1} - a \) follows immediately. If \( (a, 2) = 1 \), then by Fermat’s Little theorem, \( a^1 \equiv 1 \pmod{2} \), and raising both sides to the \( 2^p - 2 \), we obtain \( a^{2^p-2} \equiv 1 \pmod{2} \) and hence \( a^{2^p-1} \equiv a \pmod{2} \), that is \( a^{n-1} \equiv a \pmod{2} \), and thus \( 2 | a^{n-1} - a \).

Similarly, if \( (a, p) \neq 1 \), then \( p | a \), and thus \( a \equiv 0 \pmod{p} \), whence \( a^{n-1} \equiv a \pmod{p} \) and \( p | a^{n-1} - a \) follows immediately. If \( (a, p) = 1 \), then by Fermat’s Little theorem, \( a^p-1 \equiv 1 \pmod{p} \), and squaring both sides, yields \( a^{2p-2} \equiv 1 \pmod{p} \) whence \( a^{2p-1} \equiv a \pmod{p} \), that is \( a^{n-1} \equiv a \pmod{p} \), and thus \( p | a^{n-1} - a \). □

Problem 5 (15pts) Suppose that \( n \) has a primitive root. Prove that \( n \) has exactly \( \phi(\phi(n)) \) primitive roots.

Solution. Let \( a \) be a primitive root of \( n \) and let \( a_1, \ldots, a_{\phi(n)} \) be the \( \phi(n) \) incongruent elements less than or equal to \( n \) and relatively prime to \( n \). Since primitive roots have orders, but orders are only defined for relatively prime elements, the remaining primitive roots must live in \( \{a_1, \ldots, a_{\phi(n)}\} \). Since the elements of this set are incongruent modulo \( n \), it is thus enough to count the elements in \( \{a_1, \ldots, a_{\phi(n)}\} \) with order \( \phi(n) \). By a theorem from the text, we know that, modulo \( n \), \( \{a_1, \ldots, a_{\phi(n)}\} \equiv \{a, a^2, \ldots, a^{\phi(n)}\} \), and since these two collections have the same size, the elements in \( \{a, a^2, \ldots, a^{\phi(n)}\} \) are incongruent modulo \( n \). Thus it is enough to count the elements in \( \{a, a^2, \ldots, a^{\phi(n)}\} \) with order \( \phi(n) \). But the order of \( a^h \) is \( \frac{\phi(n)}{(\phi(n), h)} \), so that the primitive elements in \( \{a, a^2, \ldots, a^{\phi(n)}\} \) are those \( a^h \) such that \( \frac{\phi(n)}{(\phi(n), h)} = \phi(n) \), i.e., those for which \( (\phi(n), h) = 1 \). So it is enough to count the number of strictly positive integers \( i \leq \phi(n) \) such that \( (\phi(n), i) = 1 \). By definition, this is exactly \( \phi(\phi(n)) \), which completes the proof. □