Due date: March 2 (in the beginning of the class period)

It is ok to discuss solutions with other students but make sure to think about it first yourself. If you do discuss solutions, include a list of collaborators on your answer sheet. The writeup of the homework should be fully your own.

1. (20 points) Find a primitive root of the prime 19. Find a number between 1 and 18 that is not a primitive root of 19. (Justify your answer.)

2. (20 points) Let \( a \) and \( p \) be integers, with \( p \) being a prime. Prove that if \( a^2 \equiv 1 \pmod{p} \), then \( a \equiv 1 \pmod{p} \) or \( a \equiv -1 \pmod{p} \). Show that this need not be true if \( p \) is not a prime, by giving a counterexample.

3. (20 points) Let \( p \) be a prime and \( g \) be a primitive root of \( \mathbb{Z}_p \) (integers modulo \( p \)). Suppose that \( x = a \) and \( x = b \) are both integer solutions to the congruence \( g^x \equiv h \pmod{p} \). Prove that \( a \equiv b \pmod{p-1} \).

4. (20 points) Let \( p \) be a prime and \( g \) be a primitive root of \( \mathbb{Z}_p \). For \( h \) such that \( 1 \leq h \leq (p-1) \), let \( \log_g(h) \) denote the unique integer between 1 and \( p-1 \) such that \( g^{\log_g(h)} \equiv h \pmod{p} \). (This is the discrete log of \( h \) with respect to the primitive root \( g \)). Prove that for that for all \( h_1, h_2 \) such that \( 1 \leq h_1, h_2 \leq p-1 \),
\[
\log_g(h_1 h_2) \equiv \log_g(h_1) + \log_g(h_2) \pmod{p-1}
\]

5. (20 points) Determine whether each of the statements below is true or false (no justification needed).

(a) \( n^4 \) is \( O(n^3 + 100n^2) \)
(b) \( (\log n)^{100} \) is \( O(n^{1/100}) \)
(c) \( n^3 \cdot \log n \) is \( O\left(\frac{100n^3}{\log n}\right) \).
(d) \( x^5 \) is \( \Omega(2^x) \)
(e) \( 2^x \) is \( \Omega(x^3) \)
(f) \( 2^x \) is \( \Theta(2^{x-5}) \)
(g) \( 2^x \) is \( O(2^{x/5}) \)
(h) \( 2^x \cdot x^3 \) is \( O(3^x) \)
(i) \( 2^x \cdot x^3 \) is \( \Theta(3^x) \)
(j) \( 2^x + x^3 \) is \( \Theta(2^x) \)