Discrete Logarithms: Exercises

1. Use the table of discrete logarithms from the lecture notes to compute the following:
   (a) \( \text{ind}_{10} 6 \pmod{29} \); \( \text{ind}_{10} 16 \pmod{29} \).

2. Use the table of discrete logarithms from the lecture notes to compute the following:
   (a) \( \text{ind}_2 10 \pmod{27} \); \( \text{ind}_2 16 \pmod{25} \).

3. Use the table of discrete logarithms to solve the following congruences:
   (a) \( 3x^5 \equiv 1 \pmod{23} \); (b) \( 4x^9 \equiv 23 \pmod{31} \).

4. Use the table of discrete logarithms to solve the following congruences:
   (a) \( 2x^5 \equiv 13 \pmod{27} \); (b) \( 4x^9 \equiv 14 \pmod{25} \).

5. Use the table of discrete logarithms to find all solutions to the following congruences:
   (a) \( 3^x \equiv 2 \pmod{23} \); (b) \( 13^x \equiv 6 \pmod{23} \).

6. Show that \( x^6 \equiv 5 \pmod{17} \) has no solution, by showing that 5 is not a 6th power residue modulo 17. Is the congruence \( 2x^6 \equiv 10 \pmod{17} \) solvable?

7. Show that \( x^{15} \equiv 4 \pmod{71} \) has no solution, by showing that 4 is not a 15th power residue modulo 71.

8. Show that \( x^{15} \equiv 4 \pmod{81} \) has no solution, by showing that 4 is not a 15th power residue modulo 81.

9. Compile a list of all 4th power residues modulo 17.

10. Compile a list of all perfect squares in the ring \( \mathbb{Z}/17\mathbb{Z} \).

11. Find all solutions to \( x^x \equiv x \pmod{23} \).

12. Let \( p \) be an odd prime, and let \( r \) be a primitive root modulo \( p \). Show that \( \text{ind}_r (-1) = \text{ind}_r (p - 1) = (p - 1)/2 \).

13. Let \( p \) be an odd prime. Use the result of the preceding exercise to show that the congruence \( x^4 \equiv -1 \pmod{p} \) has a solution iff \( p \) is of the form \( 8k + 1 \).

14. What is the converse of Fermat’s Little Theorem? Show that the converse of Fermat’s Little Theorem is false, by finding integers \( a, n \) such that \( a^{n-1} \equiv 1 \pmod{n} \) and \( n \) is composite.
15. (Lucas’s Converse to FLiT, 1876) Let \( n \) be a positive integer. Suppose that an integer \( x \) can be found such that \( x^{n-1} \equiv 1 \pmod{n} \) and \( x^{(n-1)/q} \not\equiv 1 \pmod{n} \) for every prime divisor \( q \) of \( n - 1 \). Prove that \( n \) must be prime. [Hint: Argue that \( \text{ord}_n x = n - 1 \), and thus that \( \varphi(n) = n - 1 \).]

16. Apply the result of the preceding exercise, with \( x = 11 \), to show that 1009 is prime.

17. Use Lucas’s Converse to FLiT to prove that if \( n \) is an odd positive integer and there is some integer \( x \) with \( x^{(n-1)/2} \equiv -1 \pmod{n} \) and \( x^{(n-1)/q} \not\equiv 1 \pmod{n} \) for all prime divisors \( q \) of \( n - 1 \), then \( n \) must be prime.

18. Use the result of the preceding exercise, with \( x = 5 \), to prove that 2003 is prime.

19. * (Proth’s Primality Test, 1878) If \( n \) has the form \( n = k2^m + 1 \) for positive integers \( k, m \) with \( k \) odd and \( k < 2^m \), and if there is some \( x \) such that \( x^{(n-1)/2} \equiv -1 \pmod{n} \) then \( n \) must be prime. Prove this.

20. Use the result of the preceding exercise, with \( x = 3 \), to prove that 3329 is prime.