EXERCISES

1. Show that 2 is a primitive root modulo 29.
2. Compute all primitive roots for $p = 11, 13, 17$, and 19.
3. Suppose that a is a primitive root modulo p^n, p an odd prime. Show that a is a primitive root modulo p.
4. Consider a prime p of the form $4t + 1$. Show that a is a primitive root modulo p iff $-a$ is a primitive root modulo p.
5. Consider a prime p of the form $4t + 3$. Show that a is a primitive root modulo p iff $-a$ has order $(p - 1)/2$.
6. If $p = 2^n + 1$ is a Fermat prime, show that 3 is a primitive root modulo p.
7. Suppose that p is a prime of the form $8t + 3$ and that $q = (p - 1)/2$ is also a prime. Show that 2 is a primitive root modulo p.
8. Let p be an odd prime. Show that a is a primitive root module p iff $a^{(p-1)/q} \not\equiv 1\ (p)$ for all prime divisors q of $p - 1$.
9. Show that the product of all the primitive roots modulo p is congruent to $(-1)^{\phi(p-1)}$ modulo p.
10. Show that the sum of all the primitive roots modulo p is congruent to $\mu(p - 1)$ modulo p.
11. Prove that $1^k + 2^k + \cdots + (p - 1)^k \equiv 0\ (p)$ if $p - 1 \nmid k$ and $-1\ (p)$ if $p - 1 \mid k$.
12. Use the existence of a primitive root to give another proof of Wilson's theorem $(p - 1)! \equiv -1\ (p)$.
13. Let G be a finite cyclic group and $g \in G$ a generator. Show that all the other generators are of the form g^k, where $(k, n) = 1$, n being the order of G.
14. Let A be a finite abelian group and $a, b \in A$ elements of order m and n, respectively. If $(m, n) = 1$, prove that ab has order mn.
15. Let K be a field and $G \subseteq K^*$ a finite subgroup of the multiplicative group of K. Extend the arguments used in the proof of Theorem 1 to show that G is cyclic.
16. Calculate the solutions to $x^3 \equiv 1\ (19)$ and $x^4 \equiv 1\ (17)$.
17. Use the fact that 2 is a primitive root modulo 29 to find the seven solutions to $x^7 \equiv 1\ (29)$.
18. Solve the congruence $1 + x + x^2 + \cdots + x^6 \equiv 0\ (29)$.
19. Determine the numbers a such that $x^3 \equiv a\ (p)$ is solvable for $p = 7, 11$, and 13.
20. Let p be a prime and d a divisor of $p - 1$. Show that the dth powers form a subgroup of $U(\mathbb{Z}/p\mathbb{Z})$ of order $(p - 1)/d$. Calculate this subgroup for $p = 11$, $d = 5$; $p = 17$, $d = 4$; $p = 19$, $d = 6$.
21. If g is a primitive root modulo p and $d \mid p - 1$, show that $g^{(p-1)/d}$ has order d. Show also that a is a dth power iff $a \equiv g^{kd}\ (p)$ for some k. Do Exercises 16–20 making use of these observations.