Exercises 6.5

Brief solutions at end of Exercises. Complete solutions at

www.oup.co.uk/companion/NumberTheory

1. (i) Show that 3 is a primitive root of both modulo 5 and 25.
   (ii) Show that 8 is also a primitive root of both modulo 5 and 25.

2. Determine *two* incongruent primitive roots modulo 27.

3. Determine a primitive root modulo 121.

4. Verify that 10 is a primitive root modulo 49. Hence or otherwise find a primitive root of 343.

5. Show that 47 is a primitive root modulo 49.

6. (i) Show that 2 is a primitive root modulo 81.
   (ii) Show that 5 is a primitive root modulo 81.
   (ii) Show that 79 is *not* a primitive root modulo 81.

7. Which of the following integers have a primitive root?
   (a) 10 (b) 12 (c) 50 (d) 100 (e) 98 (f) 18
   (g) 22 (h) 118
   If they have primitive roots then find one of the primitive roots.

8. Determine *all* the incongruent primitive roots modulo 25.

9. Determine *all* the incongruent primitive roots modulo 49.

10. Determine *all* the incongruent primitive roots modulo 54.

{Hint: $\{2, 5, 11, 14, 20, 23\}$ are primitive roots modulo 27.}

11. Find all the *incongruent* primitive roots modulo 38.

12. Show that 14 is a primitive root modulo 29 but 14 is *not* a primitive root modulo 29^2. Find a primitive root modulo 29^2.

13. Find a primitive root modulo $2 \times 13^4 = 57\,122$.

14. Find *all* the incongruent primitive roots modulo 34.

15. (i) Show that 3 is a primitive root modulo 343.
    (ii) Solve the quadratic congruence $x^2 \equiv 295 \pmod{343}$.
    *(iii) Find *all* the incongruent solutions to $x^7 \equiv 325 \pmod{343}$.

16. Prove Lemma (6.24).

17. Prove Proposition (6.28).

18. Prove Proposition (6.29).

19. Let p be an odd prime. Prove that p^k and $2p^k$ have the same number of incongruent primitive roots.

20. *Prove Proposition (6.32) (a).
    Hint: Use mathematical induction on k.

21. *Prove Proposition (6.32) (b).

22. Let r be a primitive root of an odd prime p. Show that

$$\left(r+mp\right)^{p-1} \not\equiv 1 \left(\text{mod } p^2\right) \quad \Rightarrow \quad r+mp \text{ is a primitive root of } p^k \text{ for } k \geq 1$$

23. Show that the integer $n = 2^i p^j$ where $i \geq 2$ and $j \geq 1$ has *no* primitive roots.

24. Let $\gcd\left(r, \quad n\right) = 1$ and n have *no* primitive roots. If $r^m \equiv 1 \left(\text{mod } n\right)$ then show that in general $m \not| \ \phi\left(n\right)$.

    Hint: Consider modulo $n = 15$.

25. Let r be a primitive root of p^k where p is an odd prime and $k \geq 1$. Show that it does *not* necessarily follow $r + p$ is also a primitive root modulo p^k.

    [Hint: Consider modulo 5^2.]

26. Let r be a primitive root modulo n. Prove that the multiplicative inverse of $r \left(\text{mod } n\right)$ is *also* a primitive root modulo n.

    [Note that we have already proven this for the case $n = p$ where p is prime in question 16 of the previous Exercises 6(d).]

27. *Determine the least positive residue x such that $3^{3^8} + 1 \equiv x \left(\text{mod } 50\right)$.

Brief Solutions

2. 2 and 5
3. 2
7. (a) 7 (b) No (c) 27 (d) No (e) 3 (f) 11
   (g) 13 (h) 61
8. $\left\{2, \ 3, \ 8, \ 12, \ 13, \ 17, \ 22, \ 23\right\}$
9. $\left\{3, \ 5, \ 10, \ 12, \ 17, \ 24, \ 26, \ 33, \ 38, \ 40, \ 45, \ 47\right\}$

10. $\{5, 11, 23, 29, 41, 47\}$

11. $\{3,\ 13,\ 15,\ 21,\ 29,\ 33\}$

12. 43

13. 28563

14. $\{3, 5, 7, 11, 23, 27, 29, 31\}$

15. (ii) $148, 195 \pmod{343}$ (iii) $31, 80, 129, 178, 227, 276, 325 \pmod{343}$

26. $4 \pmod{50}$

27. $x \equiv 4 \pmod{50}$