1. Show that 3 is a primitive root modulo 34. Find all primitive roots modulo 34.

Note that $\varphi(34) = \varphi(2) \cdot \varphi(17) = 16$. So the possible orders of 3 modulo 34 are 1, 2, 4, 8, and 16. Hence, we compute

$$\begin{aligned}
3^1 &\equiv 3 \not\equiv 1 \mod 34\\
3^2 &\equiv 9 \not\equiv 1 \mod 34\\
3^4 &\equiv 81 \equiv 13 \not\equiv 1 \mod 34\\
3^8 &\equiv 169 \equiv 33 \not\equiv 1 \mod 34
\end{aligned}$$

Since the order of 3 is not equal to 1, 2, 4, or 8, we must have that the order of 3 is 16 and hence, 3 is a primitive root modulo 34.

The primitive roots modulo 34 are then $\{3^j : j \in (\mathbb{Z}/16\mathbb{Z})^\times\}$, i.e.

$$\begin{aligned}
3^1 &\equiv 3 \mod 34\\
3^3 &\equiv 27 \mod 34\\
3^5 &\equiv 5 \mod 34\\
3^7 &\equiv 11 \mod 34\\
3^9 &\equiv 31 \mod 34\\
3^{11} &\equiv 7 \mod 34\\
3^{13} &\equiv 29 \mod 34\\
3^{15} &\equiv 23 \mod 34
\end{aligned}$$

2. Show that there are no primitive roots modulo 12.

The elements of $(\mathbb{Z}/12\mathbb{Z})^\times$ are $1, 5, 7$, and 11. 1 cannot be a primitive root since the order of 1 is 1. We next observe that

$$\begin{aligned} 5^2 &\equiv 1 \mod 12 \\ 7^2 &\equiv 1 \mod 12 \\ 11^2 &\equiv 1 \mod 12 \end{aligned}$$

and so the orders of 5, 7, and 11 are all 2. Hence, $(\mathbb{Z}/12\mathbb{Z})^\times$ has no element of order $4 = \varphi(12)$. Therefore, there is no primitive root modulo 12.

3. Show that if m is a positive integer and $a \in (\mathbb{Z}\,/\,m\mathbb{Z})^\times$ with $\operatorname{ord}_m(a) = m-1$, then m is prime.

For any a, $\operatorname{ord}_m(a) \mid \varphi(m)$. Hence, $m-1 \mid \varphi(m)$. Since this implies that $m-1 \leqslant \varphi(m) < m$, we must have that $m-1 = \varphi(m)$. As a consequence, there are $m-1$ elements in $\{1, 2, \ldots, m-1\}$ which are relatively prime to m. But that means that each integer i with $1 \leqslant i \leqslant m-1$ is relatively prime to m, so in particular, m has no positive divisors other than 1 and m. Hence, m is prime.

4. Suppose that r and r' are primitive roots modulo n where $n \geqslant 3$. Show that rr' is not a primitive root modulo n.
   Hint: Use the fact that r^k is a primitive root modulo n if and only if k is relatively prime to $\varphi(n)$.

   Because r is a primitive root, there exists a k with $(k, \varphi(n)) = 1$ so that $r' = r^k$. Since $n \geqslant 3$, $\varphi(n)$ is even and since $(k, \varphi(n)) = 1$, k must be odd. Moreover $rr' = r^{k+1}$. $k + 1$ is even since k is odd and so $2 \mid k + 1$ and $2 \mid \varphi(n)$, so $2 \mid (k + 1, \varphi(n))$. Hence, $r^{k+1} = rr'$ cannot be a primitive root modulo n.

5. Does the expression $\lim_{n\to\infty} \operatorname{ord}_n(7)$ make sense? Why or why not? If it makes sense, does the limit converge? If yes, what does it converge to?

   The expression $\lim_{n\to\infty} \operatorname{ord}_n(7)$ does not make sense. For it to make sense, there must exist an N so that for all $n \geqslant N$, $\operatorname{ord}_n(7)$ is defined. However, $\operatorname{ord}_n(7)$ is defined if and only if $7 \in (\mathbb{Z} / n\mathbb{Z})^\times$. But $7 \notin (\mathbb{Z} / n\mathbb{Z})^\times$ whenever n is a multiple of 7. Since there are arbitrarily large multiples of 7, there does not exist an N so that for all $n \geqslant N$, $\operatorname{ord}_n(7)$ is defined.