3.2. **The case of odd prime powers and the general case.** We first show that primitive roots always exist for powers of odd primes. After that we wrap up and give a list of all values of $m \geqslant 2$ which possess primitive roots.

Proposition 3.8. *Let p be an odd prime and $l \geqslant 2$ an integer. Then $\mathbb{Z}_{p^l}^*$ is cyclic; i.e. there exist primitive roots modulo p^l.*

Proof. We prove the result in three steps. We first produce a candidate, then prove that it is indeed a primitive root modulo p^l.

Step 1. By Corollary 3.5, we assume g is a primitive root modulo p. Then we have $g^{p-1} \equiv 1 \pmod{p}$. We claim that we can choose g such that $g^{p-1} \not\equiv 1 \pmod{p^2}$.

In fact, if g satisfies $g^{p-1} \equiv 1 \pmod{p^2}$, we can consider $g+p$, which is still a primitive root modulo p. However we have

$$\begin{aligned}(g+p)^{p-1} &\equiv g^{p-1} + (p-1)g^{p-2}p \pmod{p^2} \\ &\equiv 1 + (p-1)g^{p-2}p \pmod{p^2} \\ &\not\equiv 1 \pmod{p^2},\end{aligned}$$

which shows that we can replace g by $g+p$ and achieve our claim.

Step 2. By Step 1 we can write $g^{p-1} \equiv 1 + ap \pmod{p^2}$ for some $a \in \mathbb{Z}$ not divisible by p. We claim that for each $l \geqslant 2$, we similarly have

$$g^{\phi(p^{l-1})} \equiv 1 + a \cdot p^{l-1} \pmod{p^l}. \tag{3.1}$$

We prove it by induction on l. When $l = 2$, the claim follows from Step 1. Assume the claim is true for some $l \geqslant 2$, then we can write

$$g^{\phi(p^{l-1})} = 1 + b \cdot p^{l-1}$$

for some $b \in \mathbb{Z}$ with $a \equiv b \pmod{p}$. Then

$$g^{\phi(p^l)} = (1 + b \cdot p^{l-1})^p = 1 + b \cdot p^l + \sum_{i=2}^{p-1} \binom{p}{i} b^i \cdot p^{i(l-1)} + b^p \cdot p^{p(l-1)}.$$

We know $\binom{p}{i}$ is divisible p. (Indeed, we have $p! = i!(p-i)!\binom{p}{i}$ by the definition of binomial coefficients. The left-hand side is divisible by p, hence so is the right-hand side. But p does not divide $i!(p-i)!$ since it is a product of integers less than, and thus coprime to p. Hence p divides $\binom{p}{i}$.) Therefore for each $i \geqslant 2$, the corresponding term in the summation is divisible by $p^{1+i(l-1)}$, where $1 + i(l-1) \geqslant 1 + 2(l-1) \geqslant l+1$. The term after the summation is divisible by $p^{p(l-1)}$, where $p(l-1) \geqslant 3(l-1) \geqslant l+1$ since p is an odd prime. Also notice that the difference of a and b is a multiple of p. All this together implies

$$g^{\phi(p^l)} \equiv 1 + a \cdot p^l \pmod{p^{l+1}}. \tag{3.2}$$

Therefore the claim is true for $l+1$.

Step 3. We show that for each $l \geqslant 2$, the order of g modulo p^l is $\phi(p^l)$; i.e. g is a primitive root modulo p^l.

Denote the order of g modulo p^l by d. First of all, $g^d \equiv 1 \pmod{p^l}$ implies $g^d \equiv 1 \pmod{p}$. Since we chose g to be a primitive root modulo p in Step 1, we know that $\phi(p)$ divides d. Then by (3.2) we have $g^{\phi(p^l)} \equiv 1 \pmod{p^l}$, hence d divides $\phi(p^l)$. Finally by (3.1) we have $g^{\phi(p^{l-1})} \not\equiv 1 \pmod{p^l}$, hence d does not divide $\phi(p^{l-1})$. These requirements leave $d = \phi(p^l)$ as the only possibility. □

Remark 3.9. Notice that Steps 2 and 3 in the proof actually shows that: if g is a primitive root modulo p and $g^{p-1} \not\equiv 1 \pmod{p^2}$, then g is a primitive root modulo p^l for any integer $l \geqslant 2$. This sufficient condition will be handy in looking for primitive roots modulo higher powers of odd primes; see Exercise 3.1 for an example. In fact, this condition is also necessary; see Exercise 3.4.

Finally we put all our existing results together and get:

Theorem 3.10. *An integer $m \geqslant 2$ possesses primitive roots iff m is of the form 2, 4, p^k or $2p^k$, where p is an odd prime and k is a positive integer.*

Proof. This proof is not covered in lecture and is non-examinable.

We first show that m possesses primitive roots if it has one of the given forms. We already know this for 2, 4 and p^k. In the last case, by Remark 2.20 we have

$$\mathbb{Z}_{2p^k}^* \cong \mathbb{Z}_2^* \times \mathbb{Z}_{p^k}^* \cong \mathbb{Z}_{p^k}^*,$$

it follows that $\mathbb{Z}_{2p^k}^*$ is cyclic; i.e. $2p^k$ possesses primitive roots.

We then show that n does not possess primitive roots in all other cases. We already know this for $m = 2^l$ with $l \geqslant 3$, so we can now assume m is not a power of 2.

We claim that m can be written as a product $m_1 m_2$, where m_1 and m_2 are coprime, $m_1 > 2$ and $m_2 > 2$. Indeed, assume $m = 2^a p_1^{a_1} p_2^{a_2} \cdots p_l^{a_l}$ is the prime factorisation of m, where $p_1, p_2, \cdots, p_l$ are distinct odd primes, $a \geqslant 0$ and $a_i \geqslant 1$ for each i. If $l \geqslant 2$, then we can take $m_1 = p_1^{a_1}$ and $m_2 = 2^a p_2^{a_2} \cdots p_l^{a_l}$. Otherwise $l = 1$, hence by assumption $a \geqslant 2$, then we can take $m_1 = 2^a$ and $m_2 = p_1^{a_1}$.

We then have that $\phi(m_1)$ and $\phi(m_2)$ are both even by Exercise 1.2 and that $\mathbb{Z}_m^* \cong \mathbb{Z}_{m_1}^* \times \mathbb{Z}_{m_2}^*$ by Remark 2.20. Since every group of even order has an element of order 2, both factors have elements of order 2, which implies that $\mathbb{Z}_m^*$ has at least two elements of order 2. Therefore it is not cyclic since a cyclic group contains at most one element of order 2. Thus m does not possess primitive roots. □