5.3: The Existence of Primitive Roots

In this section, we demonstrate which integers have primitive roots. We start by showing that every power of an odd prime has a primitive root and to do this we start by showing that every square of an odd prime has a primitive root.

If \((p)\) is an odd prime with primitive root \((r)\), then one can have either \((r)\) or \((r+p)\) as a primitive root modulo \((p^2)\).

Notice that since \((r)\) is a primitive root modulo \((p)\), then \(\text{ord}_{p^2} r\neq \phi(p^2)\). Let \(m=\text{ord}_{p^2} r\), then \(r^m \equiv 1 (mod \ p^2)\). By Theorem 54, we have \(p-1 | m\) By Exercise 7 of section 6.1, we also have that \(m | \phi(p^2)\). Also, \(\phi(p^2) = p(p-1)\) and thus \(m\) either divides \(p\) or \((p-1)\). And since \(p-1 \mid m\) then we have \((p^2) \mid m\). If \(m=p(p-1)\) then \(r^m \equiv 1 (mod \ p^2)\). Otherwise, we have \(m \equiv 1 (mod \ p^2)\) and \(r^m \equiv 1 (mod \ p^2)\). Let \((s=r+p)\). Then \((s)\) is also a primitive root modulo \((p^2)\). Hence, \(\text{ord}_{p^2} s\) equals either \((p-1)\) or \((p(p-1))\). We will show that \(\text{ord}_{p^2} s \neq 1(p-1)\) so that \(\text{ord}_{p^2} s = p(p-1)\). Note that \(s^p - p(p-1)\). Hence \(s^p = r^p + p(p-1)\). Hence \(\text{ord}_{p^2} s^p = p(p-1)\). Notice that 7 has 3 as a primitive root. Either \(\text{ord}_{49} 3 = 6\) or \(\text{ord}_{49} 3 = 42\). But since \(3 \equiv 1 (mod \ 49)\). Hence \(\text{ord}_{49} 3 = 42\). Hence 3 is a primitive root of 49.

We now show that any power of an odd prime has a primitive root.

Let \((p)\) be an odd prime. Then any power of \((p)\) is a primitive root. Moreover, if \((r)\) is a primitive root modulo \((p^2)\), then \((r)\) is a primitive root modulo \((p^m)\) for all positive integers \((m)\).
By Theorem 62, we know that any prime \( p \) has a primitive root \( r \) which is also a primitive root modulo \( p^2 \). We will prove by induction that \( \text{if} \langle 2 \rangle \equiv p \mod m, \text{then} \langle 2 \rangle \equiv r \mod (p^2-1) \) for all integers \( m \). We will prove the above congruence, we show that \( r \) is also a primitive root modulo \( p^m \). Let \( \langle n \rangle = \text{ord}_p r \). By Theorem 54, we know that \( \langle n \rangle \equiv \phi(p^m) \mod (p^m-1) \). Also, we know that \( \langle r \rangle \equiv \phi(p^m) \mod (p^m-1) \). Hence \( \langle n \rangle \mid \phi(p^m) \). On the other hand, because \( \phi(p^m) \) we also know that \( \langle n \rangle \mid \phi(p^m) \). Since \( \langle n \rangle \mid \phi(p^m) \), we see that by Theorem 54, we have \( \langle n \rangle \mid \phi(p^m) \). Also, \( \langle n \rangle \mid \phi(p^m) \), we have that \( \langle n \rangle \mid \phi(p^m) \). If \( \langle n \rangle \mid \phi(p^m) \) with \( \langle n \rangle \mid \phi(p^m) \), then \( \langle n \rangle \mid \phi(p^m) \). Hence \( \langle n \rangle \mid \phi(p^m) \).

We prove now \( \langle n \rangle \mid \phi(p^m) \) by induction. Assume that our assertion is true for all \( m \). Then \( \langle p \rangle \mid \phi(p^m) \). Because \( \langle n \rangle \mid \phi(p^m) \), we see that \( \langle n \rangle \mid \phi(p^m) \). We also know from Euler’s theorem that \( \langle p \rangle \mid \phi(p^m) \). Thus there exists an integer \( k \) such that \( \langle r \rangle \equiv 1 + kp \mod (p^m-1) \). Hence \( \langle r \rangle \mid \phi(p^m) \). Thus we have now \( \langle r \rangle \mid \phi(p^m) \). Because \( \langle r \rangle \mid \phi(p^m) \), we have \( \langle r \rangle \mid \phi(p^m) \).

Since 3 is a primitive root of 7, then 3 is a primitive root for \( \langle 7 \rangle \). In the following theorem, we prove that no power of 2, other than 2 or 4, has a primitive root and that is because when \( m \) is an odd integer, \( \langle \phi(p^m) \rangle \equiv \phi(2^m) \) and this is because \( \langle 2^m \rangle \equiv (a^{\phi(2^m)}) \).

If \( \langle m \rangle \equiv \phi(p^m) \), and if \( \langle k \rangle \equiv \phi(2^m) \), then \( \langle m \rangle \equiv \phi(2^m) \). Hence, \( \langle m \rangle \equiv \phi(p^m) \). We prove the result by induction. If \( \langle m \rangle \equiv \phi(p^m) \), then \( \langle m \rangle \equiv \phi(p^m) \). Hence, \( \langle m \rangle \equiv \phi(p^m) \). Assume now that \( \langle 2^m \rangle \equiv \phi(2^m) \). Then there is an integer \( q \) such that \( \langle m \rangle \equiv \phi(2^m) \). Thus squaring both sides, we get \( \langle m \rangle \equiv \phi(2^m) \). Thus \( \langle m \rangle \equiv \phi(2^m) \).

Note that 2 and 4 have primitive roots 1 and 3 respectively.

We now list the set of integers that do not have primitive roots.

If \( \langle m \rangle \) is not \( \langle p \rangle \) or \( \langle 2 \rangle \), then \( \langle m \rangle \) does not have a primitive root.

Let \( \langle m \rangle \equiv \langle p \rangle \), then \( \langle m \rangle \) has a primitive root \( \langle r \rangle \) and \( \langle m \rangle \) are relatively prime and \( \langle \text{ord}_m(r) \rangle \equiv \langle \text{ord}_m(p) \rangle \). We also have, we have \( \langle r \rangle \equiv \langle p \rangle \equiv \langle 2 \rangle \). By Euler’s theorem, we have \( \langle p \rangle \equiv \langle 2 \rangle \). Now let \( L = \langle \text{ord}_m(r) \rangle \equiv \langle \text{ord}_m(p) \rangle \). We know that \( \langle r \rangle \equiv \langle 2 \rangle \) and \( \langle 2 \rangle \equiv \langle 2 \rangle \). Thus using the Chinese Remainder Theorem, we get \( \langle m \rangle \equiv \langle m \rangle \). Now because \( \langle m \rangle \equiv \langle m \rangle \), we get \( \langle m \rangle \equiv \langle m \rangle \). Now the inequality above holds only if \( \langle m \rangle \equiv \langle m \rangle \).
\[m = 2p^s\] where \(p\) is an odd prime and \(t\) is any positive integer.

We now show that all integers of the form \(m = 2p^s\) have primitive roots.

Consider a prime \(p \neq 2\) and let \(s\) is a positive integer, then \(2p^s\) has a primitive root. In fact, if \(r\) is an odd primitive root modulo \(p^s\), then it is also a primitive root modulo \(2p^s\) but if \(r\) is even, \((r+p^s)\) is a primitive root modulo \(2p^s\).

If \(r\) is a primitive root modulo \(p^s\), then \([p^s] \mid (r^\phi(p^s) - 1)\] and no positive exponent smaller than \(\phi(p^s)\) has this property. Note also that \([\phi(2p^s)] = \phi(p^s)\), so that \([p^s] \mid (r^\phi(2p^s) - 1)\].

If \(r\) is odd, then \([2] \mid (r^\phi(2p^s) - 1)\]. Thus by Theorem 56, we get \([2] \mid (r^\phi(2p^s) - 1)\]. It is important to note that no smaller power of \(r\) is congruent to 1 modulo \(2p^s\). This power as well would also be congruent to 1 modulo \(p^s\) contradicting that \(r\) is a primitive root of \(p^s\). It follows that \(r\) is a primitive root modulo \(2p^s\).

While, if \(r\) is even, then \((r+p^s)\) is odd. Hence \([2] \mid ((r+p^s)^\phi(2p^s) - 1)\].

Because \([p^s] \mid (r+p^s-r)\), we see that \([p^s] \mid ((r+p^s)^\phi(2p^s) - 1)\]. As a result, we see that \([2] \mid ((r+p^s)^\phi(2p^s) - 1)\] and since for no smaller power of \((r+p^s)\) is congruent to 1 modulo \(2p^s\), we see that \((r+p^s)\) is a primitive root modulo \(2p^s\).

As a result, by Theorem 63, Theorem 65 and Theorem 66, we see that

The positive integer \(m\) has a primitive root if and only if \((n=2, 4, p^s)\) for prime \(p \neq 2\) and \(s\) is a positive integer.

**Exercises**

1. Which of the following integers 4, 12, 28, 36, 125 have a primitive root.

2. Find a primitive root of 4, 25, 18.

3. Find all primitive roots modulo 22.

4. Show that there are the same number of primitive roots modulo \(2p^s\) as there are modulo \(p^s\), where \(p\) is an odd prime and \(s\) is a positive integer.

5. Find all primitive roots modulo 25.

6. Show that the integer \(n\) has a primitive root if and only if the only solutions of the congruence \((x^2 \equiv 1 (mod n))\) are \(x \equiv \pm 1 (mod n)\).
Contributors

- Dr. Wissam Raji, Ph.D., of the American University in Beirut. His work was selected by the Saylor Foundation’s Open Textbook Challenge for public release under a Creative Commons Attribution (CC BY) license.