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 \([\text{ord}_{p}=\phi(p)=p-1] \). Let \( m=\text{ord}_{p^2} r \), then \([r^m] \equiv 1 \pmod{p^2} \). By Theorem 54, we have \([p-1] \mid m \). By Exercise 7 of section 6.1, we also have that \([m] \mid \phi(p^2) \). 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 \([m=p-1] \ \ \text{or} \ \ m=p(p-1) \). If \([m=p(p-1)] \) and \([\text{ord}_{p^2} r]=\phi(p^2) \) then \( r \) is a primitive root modulo \( p^2 \). Otherwise, we have \([m=p-1] \) and thus \([r^m] \equiv 1 \pmod{p^2} \). Let \((s=r+p) \). Then \((s)\) is also a primitive root modulo \( p \). Hence, \([\text{ord}_{p^2} s] \) equals either \([p-1] \) or \([p(p-1)] \). We will show that \([\text{ord}_{p^2} s] \neq p-1 \) so that \([\text{ord}_{p^2} s]=p(p-1) \). Note that \( (s^p) \equiv (r^p)^p \pmod{p} \). Hence \([[\text{ord}_{p^2} s]=p(p-1)] \). Note also that if \( [p^2] \mid s \) then \([\text{ord}_{p^2} s]=p(p-1) \). Thus we have \([\text{ord}_{p^2} s]=p(p-1) \). Hence \([\text{ord}_{p^2} s]=p(p-1) \). Thus, \((s=r+p) \) is a primitive root of \( p^2 \).

Notice that 7 has 3 as a primitive root. Either \([\text{ord}_{49} 3]=6 \) or \([\text{ord}_{49} 3]=42 \). But since \(3^6 \not\equiv 1 \pmod{49} \). 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 \( (r^m) \) 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 \(p^2\), thus \(\label{1} p^2 \nmid (r^{p-1}-1).\) We will prove by induction that \(\label{2} p^m \nmid (r^{p^{m-2}(p-1)}-1)\) for all integers \(m \geq 2\). Once we prove the above congruence, we show that \((r)\) is also a primitive root modulo \(p^m\). Let \(n=\text{ord}_{p^m}(r)\). By Theorem 54, we know that \(n \mid \phi(p^m)\). Also, we know that \(\phi(p^m) \equiv \phi(p^m-p^m)\). Hence \(n \mid p^m(p-1)\). On the other hand, because \(p^m \mid (r^n-1)\) we also know that \(\phi(p^m) = p^{m-1}(p-1)\). Since \(\phi(p^m) = p^{m-1}(p-1)\), we see that by Theorem 54, we have \(n \mid (p^{m-1}(p-1))\). Also \(n \mid \phi(p^m)\), we have that \(n = p^{m-1}(p-1)\). If \(n \equiv (p^{m}(s(p-1)))\) with \(s \leq m-2\), then \(p^m \mid (r^{p^m(p-2)-1})\), which is a contradiction. Hence \(n \mid \phi(p^m)\).

We prove now \((\ref{2})\) by induction. Assume that our assertion is true for all \(m \geq 2\). Then \(\phi(p^m) \equiv p^m(p-1)\) \((\mod p^m)\). Thus, \(\phi(p^m) \equiv p^m(p-1)\) \((\mod p^m)\). Since \(3\) is a primitive root of \(7\), then \(3\) is a primitive root for \(7^k\) for all positive integers \(k\).

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, \(\text{ord}_{2^k}(\phi(2^k))\) and this is because \(2^k \mid (a^\phi(2^k)/2-1)\).

If \(m\) is an odd integer, and if \(m \equiv 3\) \((\mod 4)\) is an integer, then \(m^2 \equiv 1\) \((\mod 4)\).

We prove the result by induction. If \(m\) is an odd integer, then \(m = 2n+1\) for some integer \(n\). Hence, \(m^2 = 4n^2 + 4n + 1 = 4n(2n+1) + 1\). It follows that \(8 \mid (m^2-1)\).

Assume now that \(2^k \mid (m^2-1)\). Then there is an integer \(k\) such that \(m^2 = 2^k \mid (m^2-1)\). Thus, \(2^k \mid (m^2(k-1)+1)\). Thus \(2^k \mid (m^2(k-1)+1)\) for all \(k \geq 2\).

Note now 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 \(m\) is not \(p^a\) or \(2p^a\), then \(m\) does not have a primitive root.

Let \(m = p^1 \cdot s_1 \cdot p^2 \cdot s_2 \cdot ... \cdot p_i \cdot s_i\). If \(m\) has a primitive root \(r\) then \(r\) and \(m\) are relatively prime and \(\text{ord}_{m}(r)\). We also have, we have \((r, p^a) = 1\) where \(p^a\) is of the primes in the factorization of \(m\). By Euler’s theorem, we have \(p^a \mid (r^{\phi(p^a)/2}-1)\). Now let \(L = \{\phi(p^1 \cdot s_1), \phi(p^2 \cdot s_2), ..., \phi(p_i \cdot s_i)\}\). We know that \(r^\phi \equiv 1 \mod \phi(p^a)\) for all \(1 \leq k \leq \phi(p^a)\) and \(L \leq \phi(p^a)\). Thus, using the Chinese Remainder Theorem, we get \(r^\phi \equiv 1 \mod \phi(m)\). Now because \(\phi(m) = \phi(p^1 \cdot s_1) \cdot \phi(p^2 \cdot s_2) \cdot ... \cdot \phi(p_n \cdot s_n)\) and \(L \leq \phi(m)\), we get \(r^\phi \equiv 1 \mod \phi(m)\). Now the inequality above holds only if \(\phi(p^1 \cdot s_1) = \phi(p^2 \cdot s_2) = \phi(p_n \cdot s_n)\) are relatively prime. Notice now that by Theorem 41, \(\phi(p^1 \cdot s_1), \phi(p^2 \cdot s_2), ..., \phi(p_n \cdot s_n)\) are not relatively prime unless \(m = p^a\) or
(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 \((\phi(2p^s)\mid \phi(p^s))\) 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 \((p^s)\). It follows that \((r)\) is primitive root modulo \((p^s)\).

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 \((2p^s)\mid (r+p^s)^{\phi(2p^s)}-1)\) and since 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 \((m=2p^s)\) has a primitive root if and only if \((n=2,4, p^s)\) or \((2p^s)\) 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 and Attributions

- 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.