1 Introduction

A Primitive element is a number \( a \in \mathbb{Z}_p \) given a prime \( p \) such that it has order \( p - 1 \) and therefore the following equation holds.

\[
a^{p-1} \equiv 1 \pmod{p}
\]

Importantly, there is no element \( 1 \leq k < p - 1 \) such that \( a^k \equiv 1 \pmod{p} \). The concepts presented in the study of primitive elements can be considered special cases of more general idea presented in group theory. Specifically, the primitive element \( a \) can be seen as a generator of \( \mathbb{Z}_p \), we will discuss this in more detail in the first section of the paper. Primitive elements also have applications in encryption methods, specifically the Diffie-Hellman key exchange system. Another name for primitive elements are primitive roots. Primitive elements have been studied for over two hundred years now. Leonhard Euler began studying them in the 1700s and Friedrich Gauss continued their study into the 1800s.

2 Primitive Elements in Group Theory

One important interpretation of primitive elements is that they are generators for the group \( \mathbb{Z}_p \) under multiplication[1]. The proof for the fact that \( \mathbb{Z}_p \) is a group will be omitted to save room for other content but the properties that must be proven to be true are that the group must be closed, elements must be associative, there must be an identity element, and there must be an inverse.

\[ \langle a \rangle = \mathbb{Z}_p. \]

Let \( a \) be a primitive element of the group \( \mathbb{Z}_p \). If there are \( p - 1 \) distinct elements of \( \langle a \rangle \), since all elements are in \( \mathbb{Z}_p \) due to the closed nature of groups, by the box theorem \( \langle a \rangle \) will fully populate \( \mathbb{Z}_p \). Now, for any given \( 1 \leq k, l < p - 1 \) if \( a^k \equiv a^l \pmod{p} \) then \( k \equiv l \pmod{p} \). Since \( k - l < p - 1 \) this would contradict the definition of a primitive element because there would be a number \( j = k - l \) less than \( p - 1 \) such that \( a^j \equiv 1 \pmod{p} \). This proves that every number in the set \( a, a^2, a^3, \ldots, a^{p-1} \) is unique considering the fact that \( a^{p-1} \equiv 1 \pmod{p} \) and no other number less than \( p - 1 \) and greater than zero.
can yield the same result and therefore the two sets must be equal by the box theorem, \( \langle a \rangle = \mathbb{Z}_p \). □

The concepts discussed using group theory can prove very useful when trying to prove things related to primitive elements. Although group theory is not necessarily the focus of this paper, it will prove to be a useful tool in the following proofs. It’s also worth noting that although the set of integers modulo \( n \) is denoted without the operator (*) star, this is simply notation and when using exponents it is for all intents and purposes the group of integers modulo \( n \) with the multiplication operator.

3 Concepts and Essential Proofs

Now that we have defined a primitive element, we need to know whether a primitive element exists for all primes. It turns out that yes, for every prime there is at least one primitive element[2]. A proof of this is probably outside of the scope of this paper, but this follows from theories regarding the number of roots of polynomials over finite fields. The natural question that arises next is exactly how many primitive elements exist for each prime. The proof below gives us a solid answer for this question.

Proof. There are \( \varphi(p-1) \) unique primitive elements in \( \mathbb{Z}_p \). We assume that every element of \( \mathbb{Z}_p \) can be expressed in the form \( x \equiv a^e (\text{mod } p) \) where \( a \) is a primitive element of the set, this is a corollary of the fact that primitive elements are cyclic generators on the group \( \mathbb{Z}_p \) and therefore a primitive element can express any element as an exponent of itself, we should also be able to find a \( d \) to express \( a \) as \( x^d \equiv a (\text{mod } p) \) if \( x \) is a primitive element. From here we have the substitute \( a^e \) for \( x \). We arrive at the following, \( a^{de} \equiv a (\text{mod } p) \) and \( a^{de-1} \equiv 1 (\text{mod } p) \). We want to find for how many \( e \) this equation is true such that \( de - 1 \) is of an order that is a multiple of \( p - 1 \), this would demonstrate that for a given \( e \), \( a^e \) is a primitive element. This is demonstrated by \( de - 1 \equiv 0 (\text{mod } p - 1) \) and what results is the relationship \( 1 = de - n(p - 1) \) therefore this relationship holds for any \( e \) such that we can find \( d, n \) that makes the equation 1. This is the definition of numbers \( p - 1 \) and \( e \) being relatively prime. The next question is how many numbers \( e \) can we find such they are relatively prime to \( p - 1 \), it is also important to note that \( e \) should be less than \( p - 1 \), due to the box theorem any \( e \) greater than \( p - 1 \) will be a repetition from the first \( p - 1 \) elements since they are all unique and \( \mathbb{Z}_p \) only contains \( p - 1 \) elements. This is the definition of euler’s \( \varphi \) function, so the number is \( \varphi(p-1) \). □

So, there are \( \varphi(p-1) \) elements in \( \mathbb{Z}_p \). Using the methods in this proof we can construct all primitive elements for \( \mathbb{Z}_p \) by raising it to powers that are relatively prime to \( p - 1 \). Now that we know how primitive elements behave with respect to prime numbers, a more general question would be how we apply this to \( \mathbb{Z}_n \).
for \( n \in \mathbb{N} \). For numbers that aren’t prime, we use \( \varphi(n) \) in the place of \( p - 1 \), because it is the maximum unique order of an element in \( \mathbb{Z}_n \). It turns out that not every number \( n \) possesses a primitive element in \( \mathbb{Z}_n \), but if we can generate a primitive element for this set then we will be able to construct all of the resulting primitive elements for that set. Since there is no direct way to generate a primitive element, we have to use other methods which will be discussed later in the paper. We can derive from the proof using prime numbers the number of primitive elements in \( \mathbb{Z}_n \), given that at least one primitive element exists.

**Proof.** There are \( \varphi(\varphi(n)) \) primitive elements in \( \mathbb{Z}_n \). We continue from the first proof, where \( de - 1 \equiv 0(\mod p - 1) \), instead of \( p - 1 \) however, we substitute by the more general \( \varphi(n) \) this is the generalization of \( p - 1 \) for \( n \) because it is the largest unique order that a number in \( \mathbb{Z}_n \) can have. Substituting yields the following, \( de - 1 \equiv 0(\mod \varphi(n)) \), and we seek \( d, l \) such that \( de - l\varphi(n) = 1 \). This gives us \( \varphi(\varphi(n)) \) elements that are able to satisfy this relationship. \( \square \)

As we can see, primitive elements behave similarly for arbitrary values \( n \), as long as at least one primitive element can be found in the first place. However, unlike \( \mathbb{Z}_p \), for \( \mathbb{Z}_n \) the existence of primitive elements is not guaranteed. Also, following from the proof we gave in the group theory section of the paper, it would follow that if we can prove existence of a primitive element in \( \mathbb{Z}_n \) then we can conclude that it is a cyclic group, and has several, specifically \( \varphi(\varphi(n)) \) generators.

### 4 Applications and Computation

The main application of primitive elements is in cryptography. The most well known cryptographic system that uses primitive elements is the Diffie–Hellman protocol. Just like in RSA, the goal is to share some sort of secret information over possibly monitored connections. With the Diffie–Hellman protocol we aim to create a key privately, whereas in RSA the key becomes public but only the two parties can interpret the results. In this system two numbers are initially chosen, a large prime \( p \), and one of its primitive roots \( a \). Once this is done, the agents, one and two, each pick numbers large \( x \) and \( y \) and they then compute \( X \equiv a^x(\mod p) \) and \( Y \equiv a^y(\mod p) \) respectively. Agent one sends \( X \) to agent two and agent two sends \( Y \) to agent one. Agent two calculates \( X^y \equiv a^{xy}(\mod p) \), and agent one calculates \( Y^x \equiv a^{xy}(\mod p) \) they then use \( a^{xy} \) as their key. If someone were observing their unsecured connection, the person would receive \( p, X, Y, \) and \( a \) the issue becomes how to find \( a^{xy} \) with the given information that they have[3].

It turns out that they must use some sort of algorithm to search \( k \in \mathbb{N} \) through and test whether \( a^k \) equals \( X \) or \( Y \) modulus \( p \), if they are able to find \( k \) then they have broken the code. In fact, finding \( l \) is a well known problem called a discrete logarithm problem. There are no analytic methods for calculating the...
discrete logarithm, which is one of the factors that makes this system so secure. Although there are no analytic methods, the listener may try to crack the code using numerical tests, the key here is to use very large numbers and to switch the exponents $x$ and $y$ often. So, in order to make our cryptographic system work, we must be able to generate a primitive element modulus $p$. Although there is no direct way to generate a primitive element, there are algorithms which will search for a primitive element. Below is an algorithm that will solve this problem for a prime $p$ and return $x$ which is a primitive element. We could also generalize this for any natural number, we just wouldn’t know whether a primitive element actually existed or not.

1. Compute prime factors $q_1, q_2, ..., q_n$
2. Set $x = 2$
3. Test if $x^{(p-1)/q_i} \equiv 1 \pmod{p}$
   - if it does hold for any $q_i$ then reject $x$, else break and return $x$
4. $x := x + 1$ and return to step 3

Statement 2 comes from a test of whether a number $x$ is a primitive element[4]. Notice that if 2 passes then clearly $x$ has an order less than $p−1$. To do this it tests all possible divisors of $p−1$. The listener could also come up with a similar algorithm to calculate the discrete logarithm, although most likely it is more computationally taxing. When developing an algorithm for finding primitive elements of $\mathbb{Z}_n$, it’s worth noting that there is a calculational convenience in this method, once you have tested greater than $n−\varphi(\varphi(n))$ you can conclude that no primitive elements exist, because given that one exists then you can immediately say that $\varphi(\varphi(n))$ primitive elements exist. Also, as soon as you have found one primitive element $a$, you can construct the rest using the set of numbers relatively prime to $p−1$, this makes the method of finding all primitive elements surprisingly easy.

5 Conclusion

From what we understand by doing this brief study is that many results from the theory of primitive elements are special cases of those in finite field and group theory. Things that were left unproven included the existence of primitive elements modulus for any given prime, simply because after a lot of research it seemed out of the scope of the paper and more relevant material could be provided. It’s clear that primitive elements are a deep area of study and what we gathered is that any future inquiry into the subject should probably be directed at gaining a better general knowledge of group theory and many more results could be proven.
6 References