6.8. Primitive Roots and Card Shuffling

Note. In this section, we introduce a binary algebraic structure in which we define a primitive root. We explore primitive roots and see their relationships to groups. We define the discrete logarithm and state some of its properties. We use the primitive root concept to revisit the riffle shuffle introduced in Chapter 5.

Note. Recall that for $x \equiv r \pmod{m}$, r is the *residue of* x *modulo* m and replacing a number by its residue is called *reduction mod* m; see Section 6.5. Introduction to Euler's Function.

Definition. For $m \geq 2$, define $\mathbb{Z}_m^* = \{a \in \mathbb{Z} \mid 1 \leq a \leq m \text{ and } (a, m) = 1\}$.

Note 6.8.A. For $a, b \in \mathbb{Z}_m^*$ we have $(a, m) = (b, m) = 1$ (so neither a nor b share a prime divisor with m) and therefore $(ab, m) = 1$. So multiplication on $\mathbb{Z}*_m$ followed by reduction mod m gives a commutative and associative binary operation on $\mathbb{Z}_m^*$. Since $1 \in \mathbb{Z}_m^*$, then this is an identity with respect to the binary operation. For $a \in \mathbb{Z}_m^*$ we have $(a, m) = 1$ and so by Corollary 6.21 there are integers x and y such that $ax + my = 1$, from which we have $ax \equiv 1 \pmod{m}$ and $(x, m) = 1$ (otherwise the equation $ax + my = 1$ would imply a divisor of 1 larger than 1, a contradiction). Reduction of x mod m then gives $b \in \mathbb{A}_m^*$ such that $ab \equiv 1 \pmod{m}$. Therefore each $a \in \mathbb{Z}_m^*$ has an inverse, denoted a^{-1}, with respect to the binary operation. By Theorems 6.4 and 6.6, the identity is unique and for given a the element a^{-1} is unique. We now have that $\mathbb{Z}_m^*$ is a (multiplicative) group under the (commutative) binary operation. Since $\mathbb{Z}_m^*$ only consists of elements a such that $1 \leq a \leq m$ and $(a, m) = 1$, then $\mathbb{Z}_m^*$ contains $\varphi(m)$ elements.

Note 6.8.B. The requirement that $\mathbb{Z}_m^*$ only contain $1 \leq a \leq m$ such that a is relatively prime to m, can be seen as necessary to get the group structure. For example, in $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$, elements 2, 3, and 4 have no inverses since any multiple of 0, 2, or 4 reduces modulo 6 to an even number (not to 1), and any multiple of 3 reduced modulo to either 0 or 3 (not 1).

Note 6.8.C. We use exponents to represent repeated application of the binary operation in $\mathbb{Z}_m^*$, so that $a \cdot a \cdot a \pmod{m}$ is represented as $a^3 \pmod{m}$. For repeated application of the binary operation to a^{-1} we use negative exponents, so that $a^{-1} \cdot a^{-1} \cdot a^{-1} \pmod{m}$ is represented as $a^{-3} \pmod{m}$. One can verify the usual behavior of exponents in $\mathbb{Z}_m^*$: $a^{x+y} \equiv a^x a^y \pmod{m}$ and $(a^x)^y \equiv a^{xy} \pmod{m}$. By Euler's Theorem (Theorem 6.52) we have $a^{\varphi(m)} \equiv 1 \pmod{m}$. We use this observation as motivation for the following definition.

Definition 6.73. Assume $m \geq 2$. The smallest positive integer k such that $a^k \equiv 1 \pmod{m}$ is the *order* of a modulo m, denoted $\operatorname{ord}_m a$. If $\operatorname{ord}_m a = \varphi(m)$ then a is a *primitive root modulo* m.

Theorem 6.74. If $a \in \mathbb{Z}_m^*$ and $a^t \equiv 1 \pmod{m}$, then $\operatorname{ord}_m a \mid t$. In particular, for all $a \in \mathbb{Z}_m^*$ the condition $\operatorname{ord}_m a \mid \varphi(m)$ holds.

Note. Theorem 6.74 implies that if we want to check that $a \in \mathbb{Z}_m^*$ is a primitive root modulo m, then we only need to check $a^k \pmod{m}$ for k a divisor of $\varphi(m)$ for $1 \leq k < \varphi(m)$, and not all $1 \leq k \leq \varphi(m)$ (so we need only check at most $\varphi(\varphi(m)) - 1$ values of k).

Corollary 6.75. Suppose r is a primitive root mod m. Then

(i) Every element of $\mathbb{Z}_m^*$ is congruent mod m to r^i for some i satisfying $0 \leq i \leq \varphi(m) - 1$.

(ii) If $i, j \in \mathbb{Z}$, then $r^i \equiv r^j \pmod{m}$ if and only if $i \equiv j \pmod{\varphi(m)}$.

Example 6.76. Consider $\mathbb{Z}_{14}^* = \{1, 3, 5, 9, 11, 13\}$. Since $\varphi(14) = 6$ then by Theorem 6.74 we know that $\text{ord}_m a \in \{2, 3, 6\}$ for all $a \in \mathbb{Z}_{14}^* - \{1\}$ (of course, $\text{ord}_m 1 = 1$). Checking the possible orders we have (representing equivalence modulo 14 simply as $\equiv$):

$$\begin{array}{lll} 3^2 = 9 & 3^3 = 29 \equiv 13 & 3^6 \equiv 13^2 = 169 \equiv 1 \\ 5^2 = 25 \equiv 11 & 5^3 \equiv 5 \cdot 11 = 55 \equiv 13 & 5^6 \equiv 13^2 = 169 \equiv 1 \\ 9^2 = 81 \equiv 11 & 9^3 = 9 \cdot 11 = 99 \equiv 1 & \\ 11^2 = 121 \equiv 9 & 11^3 = 11 \cdot 9 = 99 \equiv 1 & \\ 13^2 = 169 \equiv 1 & & \end{array}$$

So 3 and 5 are primitive roots mod 14, $\text{ord}_{14} 9 = \text{ord}_{14} 11 = 3$, and $\text{ord}_{14} 13 = 2$.

Note. In fact, if we take the powers of the primitive roots 3 and 5 mod 14, we find that we get all $\varphi(14) = 6$ elements of $\mathbb{Z}_{14}^* = \{1, 3, 5, 9, 11, 13\}$. This is not a coincidence, as the next result proves.

Proposition 6.77. Suppose r is a primitive root mod m. Then

(i) $\mathbb{Z}_m^*$ consists of the residues of the powers r^t with $1 \leq t \leq \varphi(m)$.

(ii) The residue of r^t is also a primitive root mod m if and only if $(t, \varphi(m)) = 1$.

Note 6.8.D. Proposition 6.77 tells us that the powers of a primitive root mod m yields all of the elements of $\mathbb{Z}_m^*$. We know that $\mathbb{Z}_m^*$ is a (multiplicative) group. In the lingo of group theory, a primitive root mod m is called a *generator* of $\mathbb{Z}_m^*$ and the group itself is said to be *cyclic*. These ideas are explored in Introduction to Modern Algebra (MATH 4127/5127). See my online notes for this class on Section I.6. Cyclic Groups; notice that Theorem 6.3 in these notes is the Division Algorithm for $\mathbb{Z}$ (which has played a big role in our congruence arithmetic).

Corollary 6.78. If primitive roots mod m exist, then there are exactly $\varphi(\varphi(m))$ of them.

Note. Recall that for real number $b > 1$, the "logarithm base b of x" is the exponent we would put on b to get x. That is, $b^{\log_b x} = x$. In $\mathbb{Z}_m^*$ we can put exponents on $a \in \mathbb{Z}_m^*$, so we have an option to define a logarithm on $\mathbb{Z}_m^*$.

Definition 6.79. Suppose a modulus m is fixed, let r be a primitive root mod m, and let $a \in \mathbb{Z}_m^*$. Consider the unique value k such that $1 \leq k \leq \varphi(m)$ and $r^k \equiv a \pmod{m}$. (By Proposition 6.77(i), we know that the powers of a "generate" $\mathbb{Z}_m^*$ and so the index k exists.) In classical number theory literature, k is the *index* of a with respect to primitive root r for the modulus m, denoted $\text{ind}_r a$. In more current literature, the number k is the *discrete logarithm* of a with respect to r, denoted $\log_r a$.

Note. The idea of an "index" is not addressed in my online notes for Elementary Number Theory (MATH 3120), but it does appear in the book I use in the course, Underwood Dudley's *Elementary Number Theory* (W. H. Freeman, 1978), in Section 23, Additional Problems, for Section 10. Primitive Roots. We now give some properties of the discrete logarithm (which are also covered in Dudley's Additional Problems section).

Proposition 6.80. Let r be a primitive root mod m, and assume that $x, y \in \mathbb{Z}_m^*$, Then

$$\log_r xy \equiv \log_r x + \log_r y \pmod{\varphi(m)}.$$

Note. By induction, we readily have the following.

Corollary 6.81. Suppose $x_1, x_2, \ldots, x_t \in \mathbb{Z}_m^*$. Then

$$\log_r x_1 x_2 \cdots x_r \equiv \sum_{i=1}^{t} \log_r x_i \pmod{\varphi(m)}.$$

Example 6.82. The number 3 is a primitive root mod 7 (since $\varphi(7) = 6$ while $3^2 \equiv 2$, $3^3 \equiv 6$, and $3^6 \equiv 1$). Computing all powers of 3 mod 7 gives (left):

n	1	2	3	4	5	6
$3^n \pmod 7$	3	2	6	4	5	1

x	1	2	3	4	5	6
$\log_3 x$	6	2	1	4	5	3

Rearranging the columns of the table on the left and letting x be the residue modulo 7 of 3^n so that $n = \log_3 x$, we get the table on the right. To illustrate the use of discrete logarithms, we compute the residue modulo 7 of the product $3 \cdot 5 \cdot 6^7$. First, we have

$$\begin{aligned} \log_3(3 \cdot 5 \cdot 6^7) &\equiv \log_3 3 + \log_3 5 + 7 \log_3 6 \pmod 6 \text{ by Corollary 6.81} \\ &\equiv 1 + 5 + 7 \cdot 3 \equiv 3 \pmod 6. \end{aligned}$$

So in $\mathbb{Z}_7^*$ we have $\log_3(3 \cdot 5 \cdot 6^7) \equiv 3$. From the table above (right), $x = 6$ satisfies $\log_3 x \equiv 3$, so we must have $3 \cdot 5 \cdot 6^7 \equiv 6 \pmod 7$.

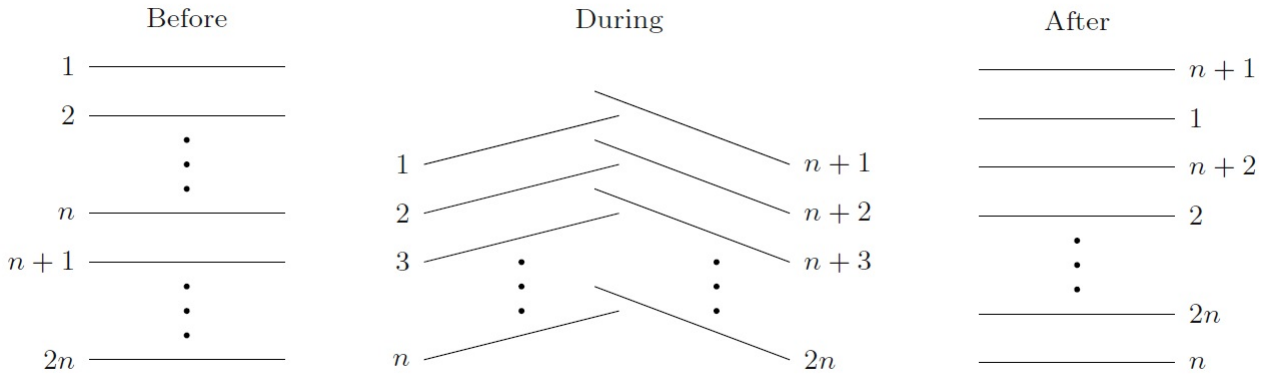
Note. It is reasonable to consider the values of m for which primitive root mod m exist. Such m are classified in the Primitive Root Theorem. A (lengthy) proof of it can be found in Amin Witno's *Theory of Numbers* online book; see his Chapter 5 Primitive Roots.

Theorem 6.83. The Primitive Root Theorem.

Suppose $m \geq 2$. Then primitive roots mod m exist if and only if m is 2 or 4 or of the form p^α or $2p^\alpha$ for some odd prime p and some $\alpha \geq 1$. In particular, primitive roots mod p exist for every prime number p.

Note. A proof of the Primitive Root Theorem (Theorem 6.83) is in my online notes for Elementary Number Theory (MATH 3120) on Section 10. Primitive Roots; see Theorem 10.6.

Note 6.8.E. We considered card shuffles in the setting of permutations in Section 5.6. We consider this idea again, but start largely from scratch (though we use a limited amount of permutation notation). Suppose we have a deck of cards with an even number $2n$ of cards. Let the cards be shuffled according the diagram:



This is called the riffle shuffle. Notice that cards initially in positions 1 through n (i.e., the top half of the deck) move from position i to position $2i$. Cards initially in positions $n+1$ through $2n$ (i.e., in the bottom half of the deck) move from position i to position $2i - (2n + 1)$ (so that the card in position $n + 1$ moves to position

1, the card in position $n+2$ moves to position 3,..., and the card in position $2n$ moves to position $2n-1$). In permutation notation (in which we list the initial positions in the first row and their new position in the second row):

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n & n+1 & n+2 & \cdots 2n-1 & 2n \\ 2 & 4 & \cdots & 2n & 1 & 3 & \cdots & 2n-3 & 2n-1 \end{pmatrix}.$$

Equivalently, the function notation is

$$\sigma(i) = \begin{cases} 2i & \text{if } 1 \le i \le n \\ 2i-(2n-1) & \text{if } n+1 \le i \le 2n. \end{cases}$$

Notice that $\sigma(i) \equiv 2i \pmod{2n+1}$ for all i, so the methods of this section may be applicable. If we perform the shuffle k times then we just iterate the function σ k times to get:

$$\sigma^k(i) \equiv 2^k i \pmod{2n+1} \text{ for } 1 \le i \le 2m.$$

We use the term "order" in the card shuffling setting as well, denoted $\operatorname{ord}\sigma$, and let this be the smallest $k \ge 1$ such that k applications of σ returns all the cards to their initial positions.

Note 6.8.F. In returning all cards to their original positions, we must return the top card (i.e., the card originally in position 1) to position 1 so we must have $\sigma^k(1) = 2^k \equiv 1 \pmod{2n+1}$. But then $\sigma^k(i) = 2^k i \equiv i \pmod{2n+1}$ for all i, and in fact $\sigma^k(i) = i$ for all i. Since we want smallest $k \ge 1$ such that $2^k \equiv 1 \pmod{2n+1}$, then in the notation of the order of an element in $\mathbb{Z}_m^*$ (see Definition 6.73), we have $k = \operatorname{ord}_{2n+1} 2$ in $\mathbb{Z}_{2n+1}^*$. That is $\operatorname{ord}\sigma = \operatorname{ord}_{2n+1} 2$. Now $2 \in \mathbb{Z}_{2n+1}^*$ and so if 2 is a primitive root of $2n+1$ then the powers of 2 include all $\varphi(2n+1)$

elements of $\mathbb{Z}^*_{2n+1}$, otherwise the powers of 2 give less than $\varphi(2n+1)$ elements of $\mathbb{Z}^*_{2n+1}$. That is, $\operatorname{ord}_{2n+1} 2 \leq \varphi(2n+1)$. Now in general, $\varphi(2n+1) \leq 2n$. Therefore, $\operatorname{ord}_{2n+1} 2 \leq \varphi(2n+1) \leq 2n$. That is, the deck will return to its original order after at most $2n$ shuffles (since $2n$ is an upper bound on $\operatorname{ord}\sigma = \operatorname{ord}_{2n+1} 2$) and is a divisor of $\varphi(2n+1)$ by Theorem 6.74.

Example 6.84. Let's consider the case of a standard deck of $2n = 52$ cards. So as described in Note 6.8.F, since $2n+1 = 53$ we have $\operatorname{ord}\sigma = \operatorname{ord}_{53} 2$. Now by Proposition 6.74, we know $\operatorname{ord}_{53} 2 \,|\, 52$. That is, $\operatorname{ord}\sigma = \operatorname{ord}_{53} 2 \in \{1, 2, 4, 13, 26, 52\}$. By considering powers of 2 we have $2^1 = 2$, $2^2 = 4$, $2^4 = 16$, $2^{13} = 2 \cdot 2^4 \cdot 2^4 \cdot 2^4 = 2 \cdot 16 \cdot 16^2 = 32 \cdot 256 \equiv 32 \cdot 44 = 1408 \equiv 30$, and $2^{26} = (2^{13})^2 \equiv 30^2 = 900 \equiv 52$. Notice that this implies $\operatorname{ord}\sigma \geq 52$, so we must have $\operatorname{ord}\sigma = 52$ (by, say, Euler's Theorem, Theorem 6.52).

Note. If we have a deck of $2n = 6$, then the permutation representing the riffle shuffle is

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 6 & 1 & 3 & 5 \end{pmatrix} = (1\ 2\ 4)(3\ 6\ 5).$$

So we see that σ^3 is the identity and so $\operatorname{ord}\sigma = 3$. We can also observe that $\operatorname{ord}_7 2 = 3$ to reach the same conclusion. Therefore the order of the riffle shuffle is not always $2n$. Let's explore the conditions under which the order of the riffle shuffle is $2n$. If $\operatorname{ord}_{2n+1} 2 = 2n$ then $\varphi(2n+1) = 2n$; that is, every positive integer less than $2n+1$ is relatively prime to $2n+1$. So $2n+1$ must be prime (by Example 6.50) and 2 is a primitive root mod $2n+1$. Conversely, if $2n+1$ is prime and 2 is a primitive root mod $2n+1$, then $\operatorname{ord}\sigma = \operatorname{ord}_{2n+1} 2 = 2n$. This gives the following.

Theorem 6.8.A. The riffle shuffle on a deck of $2n$ cards has order $2n$ if and only if $2n+1$ is prime and 2 is a primitive root mod $2n+1$.

Note. Inspired by Theorem 6.8.A, we can ask if 2 is a primitive root for infinitely many primes p. It is known by the Primitive Root Theorem that every prime has a primitive root, but it not known if there is an integer r that is a primitive root for infinitely many primes. Emil Artin, an early 20th century Austrian algebraist, conjectured that such an r exists in 1927. The conjecture has since become known as Artin's Conjecture.

Revised: 3/6/2022