Mathematical Reasoning

Chapter 6. Number Theory

6.8. Primitive Roots and Card Shuffling—Proofs of Theorems

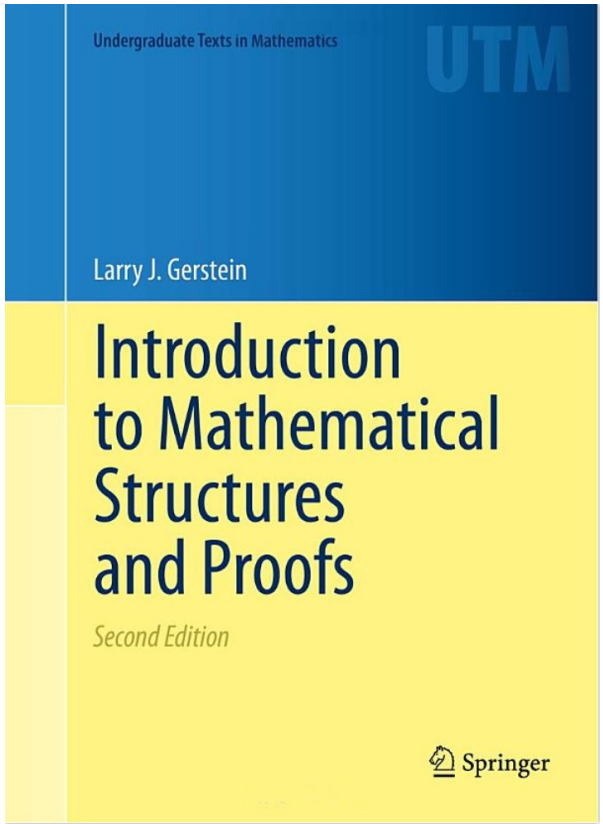

Table of contents

Theorem 6.74

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.

Proof. Let $k = \operatorname{ord}_, a$. By the Division Algorithm (Theorem 6.17) there are integers q an r such that $t = kq + r$ with $0 \leq r < k$. Then by Note 6.8.C,

$$1 \equiv q^t \equiv (a^k)^q \cdot a^r \equiv (1) \cdot a^r \equiv a^r \pmod{m}.$$

Since $k = \operatorname{ord}_m a$ is the smallest positive integer such that $a^k \equiv 1 \pmod{m}$ and $0 \leq r < l$, then we must have $r = 0$. That is, $t = kq$ and so $\operatorname{ord}_m a \mid t$, as claimed.

Theorem 6.74

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.

Proof. Let $k = \operatorname{ord}_, a$. By the Division Algorithm (Theorem 6.17) there are integers q an r such that $t = kq + r$ with $0 \leq r < k$. Then by Note 6.8.C,

$$1 \equiv q^t \equiv (a^k)^q \cdot a^r \equiv (1) \cdot a^r \equiv a^r \pmod{m}.$$

Since $k = \operatorname{ord}_m a$ is the smallest positive integer such that $a^k \equiv 1 \pmod{m}$ and $0 \leq r < l$, then we must have $r = 0$. That is, $t = kq$ and so $\operatorname{ord}_m a \mid t$, as claimed.

Since Euler's Theorem (Theorem 6.52) implies that $a^{\varphi(m)} \equiv 1 \pmod{m}$, the first result implies that $\operatorname{ord}_m a \mid \varphi(m)$, as claimed. □

Theorem 6.74

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.

Proof. Let $k = \operatorname{ord}_, a$. By the Division Algorithm (Theorem 6.17) there are integers q an r such that $t = kq + r$ with $0 \leq r < k$. Then by Note 6.8.C,

$$1 \equiv q^t \equiv (a^k)^q \cdot a^r \equiv (1) \cdot a^r \equiv a^r \pmod{m}.$$

Since $k = \operatorname{ord}_m a$ is the smallest positive integer such that $a^k \equiv 1 \pmod{m}$ and $0 \leq r < l$, then we must have $r = 0$. That is, $t = kq$ and so $\operatorname{ord}_m a \mid t$, as claimed.

Since Euler's Theorem (Theorem 6.52) implies that $a^{\varphi(m)} \equiv 1 \pmod{m}$, the first result implies that $\operatorname{ord}_m a \mid \varphi(m)$, as claimed. □

Corollary 6.75

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 $i \equiv j \pmod{\varphi(m)}$.

Proof. **(i)** Let $0 \leq i < j \leq \varphi(m) - 1$. Then for $i = j$ we have $r^i \equiv r^j \pmod{m}$ (trivially). ASSUME $r^i \equiv r^j \pmod{m}$. Then by Note 6.8.C $r^{j-i} \equiv 1 \pmod{m}$. But since r is a primitive root mod m, then $\operatorname{ord}_m a = \varphi(m)$, but $0 < j - i < \varphi(m)$, a CONTRADICTION.

Corollary 6.75

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 $i \equiv j \pmod{\varphi(m)}$.

Proof. (i) Let $0 \leq i < j \leq \varphi(m) - 1$. Then for $i = j$ we have $r^i \equiv r^j \pmod{m}$ (trivially). ASSUME $r^i \equiv r^j \pmod{m}$. Then by Note 6.8.C $r^{j-i} \equiv 1 \pmod{m}$. But since r is a primitive root mod m, then $\text{ord}_m a = \varphi(m)$, but $0 < j - i < \varphi(m)$, a CONTRADICTION. So $r^i \equiv r^j \pmod{m}$ for $0 \leq i < j \leq \varphi(m) - 1$ if and only if $i = j$. Therefore, each of the $\varphi(m)$ elements of $\mathbb{Z}_m^*$ are congruent mod m to some r^i where $0 \leq i \leq \varphi(m) - 1$, as claimed.

Corollary 6.75

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 $i \equiv j \pmod{\varphi(m)}$.

Proof. (i) Let $0 \leq i < j \leq \varphi(m) - 1$. Then for $i = j$ we have $r^i \equiv r^j \pmod{m}$ (trivially). ASSUME $r^i \equiv r^j \pmod{m}$. Then by Note 6.8.C $r^{j-i} \equiv 1 \pmod{m}$. But since r is a primitive root mod m, then $\text{ord}_m a = \varphi(m)$, but $0 < j - i < \varphi(m)$, a CONTRADICTION. So $r^i \equiv r^j \pmod{m}$ for $0 \leq i < j \leq \varphi(m) - 1$ if and only if $i = j$. Therefore, each of the $\varphi(m)$ elements of $\mathbb{Z}_m^*$ are congruent mod m to some r^i where $0 \leq i \leq \varphi(m) - 1$, as claimed.

Corollary 6.75 (continued)

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 $i \equiv j \pmod{\varphi(m)}$.

Proof (continued). (b) Without loss of generality, suppose $i \geq j$. By Note 6.8.C, the congruence $r^i \equiv r^j \pmod{m}$ is equivalent to the congruence $r^{j-i} \equiv 1 \pmod{m}$. Since r is a primitive root mod m, then $\operatorname{ord}_m r = \varphi(m)$ By Proposition 6.74, $\operatorname{ord}_m r \,|\, (j - i)$ or $\varphi(m) \,|\, (j - i)$. That is, $i \equiv j \pmod{\varphi(m)}$.

Corollary 6.75 (continued)

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 $i \equiv j \pmod{\varphi(m)}$.

Proof (continued). (b) Without loss of generality, suppose $i \geq j$. By Note 6.8.C, the congruence $r^i \equiv r^j \pmod{m}$ is equivalent to the congruence $r^{j-i} \equiv 1 \pmod{m}$. Since r is a primitive root mod m, then $\text{ord}_m r = \varphi(m)$ By Proposition 6.74, $\text{ord}_m r \,|\, (j-i)$ or $\varphi(m) \,|\, (j-i)$. That is, $i \equiv j \pmod{\varphi(m)}$. Conversely, if $i \equiv j \pmod{\varphi(m)}$ then $i = j + k\varphi(m)$ for some integer k. Then by Note 6.8.C and Euler's Theorem (Theorem 6.52) we have $r^i = r^{j+k\varphi(m)} = r^j \cdot r^{\varphi(m)} \equiv r^j \cdot (1) \equiv r^j \pmod{m}$. That is, $r^i \equiv r^j \pmod{m}$ if and only if $i \equiv j \pmod{m}$, as claimed. □

Corollary 6.75 (continued)

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 $i \equiv j \pmod{\varphi(m)}$.

Proof (continued). (b) Without loss of generality, suppose $i \geq j$. By Note 6.8.C, the congruence $r^i \equiv r^j \pmod{m}$ is equivalent to the congruence $r^{j-i} \equiv 1 \pmod{m}$. Since r is a primitive root mod m, then $\text{ord}_m r = \varphi(m)$ By Proposition 6.74, $\text{ord}_m r \,|\, (j-i)$ or $\varphi(m) \,|\, (j-i)$. That is, $i \equiv j \pmod{\varphi(m)}$. Conversely, if $i \equiv j \pmod{\varphi(m)}$ then $i = j + k\varphi(m)$ for some integer k. Then by Note 6.8.C and Euler's Theorem (Theorem 6.52) we have $r^i = r^{j+k\varphi(m)} = r^j \cdot r^{\varphi(m)} \equiv r^j \cdot (1) \equiv r^j \pmod{m}$. That is, $r^i \equiv r^j \pmod{m}$ if and only if $i \equiv j \pmod{m}$, as claimed. □

Proposition 6.77

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 $(t, \varphi(m)) = 1$.

Proof. (i) Since $r \in \mathbb{Z}_m^*$ then $(r, m) = 1$ and so r and m share no common prime divisors. So $(r^t, m) = 1$ for all $t \in \mathbb{N}$ and hence $r^t \in \mathbb{Z}_m^*$ for all $1 \leq t \leq \varphi(m)$. Suppose $1 \leq i < j \leq \varphi(m)$ and ASSUME $r^i \equiv r^j \pmod{m}$. Let $r^{-1} = s \in \mathbb{Z}_m^*$. Then by Note 6.8.C,

$$1 \equiv r^i s^i = r^j s^i \equiv r^{j-i} r^i s^i \equiv r^{j-i} \pmod{m}.$$

Proposition 6.77

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 $(t, \varphi(m)) = 1$.

Proof. (i) Since $r \in \mathbb{Z}_m^*$ then $(r, m) = 1$ and so r and m share no common prime divisors. So $(r^t, m) = 1$ for all $t \in \mathbb{N}$ and hence $r^t \in \mathbb{Z}_m^*$ for all $1 \leq t \leq \varphi(m)$. Suppose $1 \leq i < j \leq \varphi(m)$ and ASSUME $r^i \equiv r^j \pmod{m}$. Let $r^{-1} = s \in \mathbb{Z}_m^*$. Then by Note 6.8.C,

$$1 \equiv r^i s^i = r^j s^i \equiv r^{j-i} r^i s^i \equiv r^{j-i} \pmod{m}.$$

But $1 \leq j - i < \varphi(m) = \operatorname{ord}_m r$, CONTRADICTING the fact that r is a primitive root mod m and so $\operatorname{ord}_m a = \varphi(m)$. So the assumption that $r^i \equiv r^j \pmod{m}$ is false. That is, reduction mod m of r^t, where $1 \leq t \leq \varphi(m)$, includes all $\varphi(m)$ elements of $\mathbb{Z}_m^*$, as claimed.

Proposition 6.77

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 $(t, \varphi(m)) = 1$.

Proof. (i) Since $r \in \mathbb{Z}_m^*$ then $(r, m) = 1$ and so r and m share no common prime divisors. So $(r^t, m) = 1$ for all $t \in \mathbb{N}$ and hence $r^t \in \mathbb{Z}_m^*$ for all $1 \leq t \leq \varphi(m)$. Suppose $1 \leq i < j \leq \varphi(m)$ and ASSUME $r^i \equiv r^j \pmod{m}$. Let $r^{-1} = s \in \mathbb{Z}_m^*$. Then by Note 6.8.C,

$$1 \equiv r^i s^i = r^j s^i \equiv r^{j-i} r^i s^i \equiv r^{j-i} \pmod{m}.$$

But $1 \leq j - i < \varphi(m) = \operatorname{ord}_m r$, CONTRADICTING the fact that r is a primitive root mod m and so $\operatorname{ord}_m a = \varphi(m)$. So the assumption that $r^i \equiv r^j \pmod{m}$ is false. That is, reduction mod m of r^t, where $1 \leq t \leq \varphi(m)$, includes all $\varphi(m)$ elements of $\mathbb{Z}_m^*$, as claimed.

Proposition 6.77 (continued 1)

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 $(t, \varphi(m)) = 1$.

Proof (continued). (ii) First, suppose $(t, \varphi(m)) = 1$. Then by Corollary 6.21, there are integers x and y such that $1 = tx + \varphi(m)y$. Therefore by Note 6.8.C and Euler's Theorem (Theorem 6.52),

$$r = r^{tx+\varphi(m)y} = r^{tx} \cdot (r^{\varphi(m)})^y \equiv (r^t)^x \cdot (1) \pmod{m}.$$

So r is congruent to a power of r^t. Since every element of $\mathbb{Z}_m^*$ is a power of r by part (i), then every element of $\mathbb{Z}_m^*$ is a power of r^t mod m. That is, r^t is a primitive root mod m. So if $(t, \varphi(m)) = 1$ then r^t is a primitive root for any $1 \leq t \leq \varphi(m)$, as claimed.

Proposition 6.77 (continued 1)

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 $(t, \varphi(m)) = 1$.

Proof (continued). (ii) First, suppose $(t, \varphi(m)) = 1$. Then by Corollary 6.21, there are integers x and y such that $1 = tx + \varphi(m)y$. Therefore by Note 6.8.C and Euler's Theorem (Theorem 6.52),

$$r = r^{tx+\varphi(m)y} = r^{tx} \cdot (r^{\varphi(m)})^y \equiv (r^t)^x \cdot (1) \pmod{m}.$$

So r is congruent to a power of r^t. Since every element of $\mathbb{Z}_m^*$ is a power of r by part (i), then every element of $\mathbb{Z}_m^*$ is a power of r^t mod m. That is, r^t is a primitive root mod m. So if $(t, \varphi(m)) = 1$ then r^t is a primitive root for any $1 \leq t \leq \varphi(m)$, as claimed.

Proposition 6.77 (continued 2)

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 $(t, \varphi(m)) = 1$.

Proof (continued). Conversely, if the residue of r^t is a primitive root then $(r^t)^k \equiv r \pmod{m}$ for some $k \geq 1$ and therefore $r^{tk-1} \equiv 1 \pmod{m}$. Then by Proposition 6.74 gives $\operatorname{ord}_m r \mid (tk-1)$. Since r is a primitive root mod m by hypothesis, then $\operatorname{ord}_m r = \varphi(m)$. So $(tk-1)$ is a multiple of $\varphi(m)$ and $1 = tk + x\varphi(m)$ for some integer x. Thus $(t, \varphi(m)) = 1$ (since any common divisor of t and $\varphi(m)$ would be a divisor of 1). So if r^t is a primitive root mod m, then $(t, \varphi(m)) = 1$, as claimed. □

Proposition 6.77 (continued 2)

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 $(t, \varphi(m)) = 1$.

Proof (continued). Conversely, if the residue of r^t is a primitive root then $(r^t)^k \equiv r \pmod{m}$ for some $k \geq 1$ and therefore $r^{tk-1} \equiv 1 \pmod{m}$. Then by Proposition 6.74 gives $\operatorname{ord}_m r \mid (tk-1)$. Since r is a primitive root mod m by hypothesis, then $\operatorname{ord}_m r = \varphi(m)$. So $(tk-1)$ is a multiple of $\varphi(m)$ and $1 = tk + x\varphi(m)$ for some integer x. Thus $(t, \varphi(m)) = 1$ (since any common divisor of t and $\varphi(m)$ would be a divisor of 1). So if r^t is a primitive root mod m, then $(t, \varphi(m)) = 1$, as claimed. □

Proposition 6.80

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

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

Proof. By the definition of discrete logarithm, we have

$$r^{\log_r xy} \equiv xy \equiv r^{\log_r x} \cdot r^{\log_r y} \equiv r^{\log_r x + \log_r y} \pmod{m}.$$

By Corollary 6.75(ii), we have $\log_r xy \equiv \log_r x + \log_r y \pmod{\varphi(m)}$, as claimed. □

Proposition 6.80

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

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

Proof. By the definition of discrete logarithm, we have

$$r^{\log_r xy} \equiv xy \equiv r^{\log_r x} \cdot r^{\log_r y} \equiv r^{\log_r x + \log_r y} \pmod{m}.$$

By Corollary 6.75(ii), we have $\log_r xy \equiv \log_r x + \log_r y \pmod{\varphi(m)}$, as claimed. □