5. Primitive roots

5.1 Powers of integers

Let m be a positive integer and a be an integer with $(a,m) = 1$. Let $k \geq 0$ be a nonnegative integer.

(i) For nonnegative powers of a, we know that a^k is an integer, and hence we may directly determine the residue class of a^k modulo m.

(ii) For negative powers of a, we recall from Definition 3.3 that there exists an integer $\bar{a}$ such that $a\bar{a} \equiv 1 \pmod{m}$. Thus, we may use a^{-1} to represent the residue class of $\bar{a}$ modulo m. In particular, we have $aa^{-1} \equiv 1 \pmod{m}$, which is a natural analogy to the usual inverse of integers; this explains why we call $\bar{a}$ the modular inverse of a in Definition 3.3. Now, we may naturally define negative powers of a modulo m by $a^{-k} \equiv (a^{-1})^k \pmod{m}$.

R Note that if a is such that $(a,m) > 1$, then there is no integer $\bar{a}$ such that $a\bar{a} \equiv 1 \pmod{m}$, since by Theorem 2.5, $ax - 1 = my$ has no integer solutions (x,y). Thus, we cannot define negative powers of a modulo m in this case. However, nonnegative powers of a can be defined as the normal powers.

From the above definition, we have the following trivial fact.

Theorem 5.1 Let m be a positive integer and a,b be integers with $(a,m) = (b,m) = 1$ and $a \equiv b \pmod{m}$. Then for any integer x,

$$a^x \equiv b^x \pmod{m}. \tag{5.1}$$

The next two results show that integer powers in the modular sense have similar properties to normal powers of integers.

Theorem 5.2 Let m be a positive integer and a,b be integers with $(a,m) = (b,m) = 1$. Then for any integer x,

$$(ab)^x \equiv a^x b^x \pmod{m}. \tag{5.2}$$

Proof. If $x \geq 0$, then $(ab)^x = a^x b^x$ as normal integer powers, and hence they are congruent modulo m. If $x<0$, we first note that $(ab)^{-1}\equiv a^{-1}b^{-1} \pmod m$ for

$$(ab)\cdot(a^{-1}b^{-1})=(aa^{-1})\cdot(bb^{-1})\equiv 1\cdot 1=1 \pmod m.$$

Thus,

$$(ab)^x\equiv\left((ab)^{-1}\right)^{-x}\equiv(a^{-1}b^{-1})^{-x}=(a^{-1})^{-x}(b^{-1})^{-x}\equiv a^xb^x \pmod m,$$

as desired. ∎

Theorem 5.3 Let m be a positive integer and a be an integer with $(a,m)=1$. Then

(i) $1^{-1}\equiv 1 \pmod m$;
(ii) $(a^{-1})^{-1}\equiv a \pmod m$;
(iii) For any integers x and y, we have $a^{x+y}\equiv a^xa^y \pmod m$;
(iv) For any integers x and y, we have $a^{xy}\equiv (a^x)^y \pmod m$.

Proof. (i). Note that $1\cdot 1\equiv 1 \pmod m$, and hence $1^{-1}\equiv 1 \pmod m$.

(ii). Note that a^{-1} is the modular inverse of a modulo m and vice versa by definition. This means that $(a^{-1})^{-1}\equiv a \pmod m$.

(iii). This relation is trivial if x and y are simultaneously nonnegative, or simultaneously nonpositive. Without loss of generality, we assume that $x>0>y$. In particular, we may further assume that $x+y\ge 0$, for if $x+y<0$, we only need to rewrite the congruence as $(a^{-1})^{-(x+y)}\equiv(a^{-1})^{-x}(a^{-1})^{-y} \pmod m$. Now, we note that $a^x=a^{x+y-y}=a^{x+y}a^{-y}$ for both $x+y$ and $-y$ are nonnegative integers. Hence,

$$a^x\cdot a^y=(a^{x+y}a^{-y})\cdot a^y\equiv(a^{x+y}a^{-y})\cdot(a^{-1})^{-y}=a^{x+y}\cdot(a\cdot a^{-1})^{-y}\equiv a^{x+y}\cdot 1^{-y}=a^{x+y} \pmod m.$$

(iv). We require three basic facts. Firstly, for x and y nonnegative integers,

$$(a^x)^y=a^{xy}; \tag{5.3}$$

this is a property of normal integer powers. Secondly, for x a nonnegative integer,

$$(a^{-1})^x\equiv a^{-x} \pmod m; \tag{5.4}$$

this follows from the definition of negative powers in the modular sense. Thirdly, for x an integer,

$$(a^x)^{-1}=a^{-x}; \tag{5.5}$$

this follows from Part (iii) as $a^xa^{-x}\equiv a^{x+(-x)}=a^0=1 \pmod m$, namely, a^{-x} is the modular inverse of a^x. Now, we prove Part (iv) according to the following four cases. **(a).** If $x,y\ge 0$, then by (5.3) $a^{xy}=(a^x)^y$ and thus they are congruent modulo m. **(b).** If $x\ge 0>y$, then

$$(a^x)^y\overset{(5.4)}{\equiv}\left((a^x)^{-1}\right)^{-y}\overset{(5.5)}{\equiv}(a^{-x})^{-y}\overset{(5.4)}{\equiv}\left((a^{-1})^x\right)^{-y}\overset{(5.3)}{=}(a^{-1})^{-xy}\overset{(5.4)}{\equiv}a^{xy} \pmod m.$$

(c). If $y\ge 0>x$, then

$$(a^x)^y\overset{(5.4)}{\equiv}\left((a^{-1})^{-x}\right)^y\overset{(5.3)}{=}(a^{-1})^{-xy}\overset{(5.4)}{\equiv}a^{xy} \pmod m.$$

(d). If $x,y<0$, then

$$(a^x)^y\overset{(5.4)}{\equiv}\left((a^x)^{-1}\right)^{-y}\overset{(5.5)}{\equiv}(a^{-x})^{-y}\overset{(5.3)}{=}a^{xy} \pmod m.$$

The desired result hence holds true. ∎

5.2 Orders

By the Fermat–Euler Theorem (Theorem 4.6), we have $a^{\phi(m)} \equiv 1 \pmod{m}$, indicating that there exists at least one positive integer x such that $a^x \equiv 1 \pmod{m}$.

Definition 5.1 Let m be a positive integer and a be an integer with $(a,m) = 1$. The smallest positive integer d such that

$$a^d \equiv 1 \pmod{m} \tag{5.6}$$

is called the *order of a modulo m*, denoted by $\operatorname{ord}_m a$.

Example 5.1 (i). We have $\operatorname{ord}_5 2 = 4$ for $2^1 \equiv 2$, $2^2 \equiv 4$, $2^3 \equiv 3$ and $2^4 \equiv 1 \pmod{5}$. (ii). We have $\operatorname{ord}_7 2 = 3$ for $2^1 \equiv 2$, $2^2 \equiv 4$ and $2^3 \equiv 1 \pmod{7}$. ■

Theorem 5.4 Let m be a positive integer and a be an integer with $(a,m) = 1$. Then an integer x satisfies $a^x \equiv 1 \pmod{m}$ if and only if $\operatorname{ord}_m a \mid x$. In particular, $\operatorname{ord}_m a \mid \phi(m)$.

Proof. Let $d = \operatorname{ord}_m a$. Then $a^d \equiv 1 \pmod{m}$ by definition. If $d \mid x$, then we may write $x = q \cdot d$ and thus,

$$a^x = a^{qd} \equiv (a^d)^q \equiv 1^q = 1 \pmod{m}.$$

Assume that there exists an x with $d \nmid x$ such that $a^x \equiv 1 \pmod{m}$. Thus, we may write $x = q \cdot d + r$ for q and r integers with $0 < r < d$. It follows that

$$1 \equiv a^x = a^{qd+r} \equiv a^{qd} \cdot a^r \equiv (a^d)^q \cdot a^r \equiv 1 \cdot a^r = a^r \pmod{m}.$$

But this violates the assumption that d is the smallest positive integer such that $a^d \equiv 1 \pmod{m}$. Finally, $\operatorname{ord}_m a \mid \phi(m)$ since $a^{\phi(m)} \equiv 1 \pmod{m}$ by the Fermat–Euler Theorem. ■

Theorem 5.5 Let m be a positive integer and a be an integer with $(a,m) = 1$. If we write $d = \operatorname{ord}_m a$, then for any integer k,

$$\operatorname{ord}_m a^k = \frac{d}{(d,k)}. \tag{5.7}$$

In particular, for any positive d^* with $d^* \mid d$, we have $\operatorname{ord}_m a^{\frac{d}{d^*}} = d^*$.

Proof. We write $d' = \operatorname{ord}_m a^k$ and $\delta = (d,k)$. First, noting that $(a^k)^{\frac{d}{\delta}} = (a^d)^{\frac{k}{\delta}} \equiv 1^{\frac{k}{\delta}} = 1 \pmod{m}$, we have $d' \mid \frac{d}{\delta}$ by Theorem 5.4. Also, $a^{kd'} = (a^k)^{d'} \equiv 1 \pmod{m}$, and therefore $d \mid kd'$ by Theorem 5.4, implying that $\frac{d}{\delta} \mid \frac{k}{\delta} d'$. Further, we have $(\frac{d}{\delta}, \frac{k}{\delta}) = 1$ since $\delta = (d,k)$. Hence, $\frac{d}{\delta} \mid d'$. It follows that $d' = \frac{d}{\delta}$. Finally, we choose $k = \frac{d}{d^*}$ and note that $(d, \frac{d}{d^*}) = \frac{d}{d^*}$, thereby getting the last part. ■

Theorem 5.6 Let m be a positive integer and a,b be integers with $(a,m) = (b,m) = 1$. Let $d_a = \operatorname{ord}_m a$ and $d_b = \operatorname{ord}_m b$. If $(d_a,d_b) = 1$, then $\operatorname{ord}_m(ab) = d_a d_b$.

Proof. Let $d = \operatorname{ord}_m(ab)$. First, noting that $(ab)^{d_a d_b} = (a^{d_a})^{d_b} \cdot (b^{d_b})^{d_a} \equiv 1^{d_b} \cdot 1^{d_a} = 1 \pmod{m}$, we have $d \mid d_a d_b$. Also, $a^{dd_b} = a^{dd_b} \cdot 1^d \equiv a^{dd_b} \cdot (b^{d_b})^d = (ab)^{dd_b} = \big((ab)^d\big)^{d_b} \equiv 1^{d_b} = 1 \pmod{m}$, and thus $d_a \mid dd_b$. Noting further that $(d_a,d_b) = 1$, we have $d_a \mid d$. Similarly, $d_b \mid d$ and thus $d_a d_b \mid d$ since $(d_a,d_b) = 1$. It follows that $d = d_a d_b$. ■

Theorem 5.7 Let m be a positive integer and $\{a_1, a_2, \ldots, a_{\phi(m)}\}$ be a reduced residue system modulo m. Let $d_i = \operatorname{ord}_m a_i$ for $1 \le i \le \phi(m)$ and define $D = \max_{1 \le i \le \phi(m)}\{d_i\}$. Then $D \mid \phi(m)$, and $d_i \mid D$ for each $1 \le i \le \phi(m)$.

Proof. First, $D \mid \phi(m)$ follows from Theorem 5.4 and the fact that D is the order of a certain a_i, say x. For the second part, we prove by contradiction. Assume that there exists a y such that $d = \operatorname{ord}_m y \nmid D$. If we write in the canonical form $d = \prod_i p_i^{\alpha_i}$ and $D = \prod_i p_i^{\beta_i}$, then there exists at least one index i such that $\alpha_i > \beta_i$ since $d \nmid D$. Then $\operatorname{lcm}(d, D) > D$ as $\operatorname{lcm}(d, D) = \prod_i p_i^{\max(\alpha_i, \beta_i)}$. Now, we define $d' = \prod_{k: \alpha_k > \beta_k} p_k^{\alpha_k}$ and $D' = \prod_{\ell: \beta_\ell \ge \alpha_\ell} p_\ell^{\beta_\ell}$. Then $d' \mid d$, $D' \mid D$, $(d', D') = 1$ and $d'D' = \operatorname{lcm}(d, D)$. By Theorem 5.5, there exists an a of order d' and a b of order D'. Thus, by Theorem 5.6, $\operatorname{ord}_m(ab) = d'D' = \operatorname{lcm}(d, D) > D$. But this violates the fact that D is the maximum among the orders. ■

5.3 Primitive roots

Recall that the orders modulo m are always divisors of $\phi(m)$. We now focus on the case where the order equals $\phi(m)$.

Definition 5.2 An integer g is called a *primitive root* of m if $\operatorname{ord}_m g = \phi(m)$.

Theorem 5.8 If m has a primitive root g, then $\{g, g^2, \ldots, g^{\phi(m)}\}$ gives a reduced residue system modulo m.

R If m has a primitive root, then the multiplicative group $\mathbb{Z}_m^\times$ is cyclic.

Proof. Note that the $\phi(m)$ integers g, ..., $g^{\phi(m)}$ are coprime to m since $(g, m) = 1$. Hence, it suffices to show that they are pairwise distinct modulo m. Assume not; then there are integers i and j with $1 \le i < j \le \phi(m)$ such that $g^i \equiv g^j \pmod{m}$, or $g^{j-i} \equiv 1 \pmod{m}$. But g is a primitive root of m, and thus $\operatorname{ord}_m g = \phi(m)$. By Theorem 5.4, $\phi(m) \mid (j - i)$, which is impossible. ■

Theorem 5.9 If m has a primitive root, then there are $\phi(\phi(m))$ primitive roots among $1, 2, \ldots, m$.

Proof. Let g be a primitive root of m and hence $\operatorname{ord}_m g = \phi(m)$. Then Theorem 5.8 tells us that the reduced system modulo m can be represented by $\{g, \ldots, g^{\phi(m)}\}$. Thus, it suffices to determine the number of i's with $1 \le i \le \phi(m)$ such that $\operatorname{ord}_m g^i = \phi(m)$. On the other hand, we know from Theorem 5.5 that $\operatorname{ord}_m g^i = \frac{\phi(m)}{(i, \phi(m))}$. So we only need to count the number of i's such that $(i, \phi(m)) = 1$ and there are $\phi(\phi(m))$ such i's among $1, \ldots, \phi(m)$. ■

5.4 Lagrange's polynomial congruence theorem

Here, we present a theorem of Lagrange, which will be a key for confirming the existence of primitive roots of an odd prime.

Theorem 5.10 (Lagrange's Polynomial Congruence Theorem). Let p be a prime. Let $f(x) = a_n x^n + \cdots + a_1 x + a_0$ be a polynomial with integer coefficients such that $p \nmid a_n$. Then the congruence

$$f(x) \equiv 0 \pmod{p}$$

has at most n solutions modulo p.

Proof. We prove by induction on the degree n of $f(x)$. When $n = 1$, $f(x)$ is linear and the statement is trivial. Now we assume that the statement is true for $1, \ldots, n$ with $n \geq 1$. Let $f(x)$ be of degree $n+1$. If $f(x) \equiv 0 \pmod{p}$ has no solutions, then there is nothing to prove. If there is one solution, say $x \equiv x_0 \pmod{p}$, then $f(x_0) \equiv 0 \pmod{p}$. Now, we consider $g(x) = f(x) - f(x_0) = (x - x_0)q(x)$ where $q(x)$ is a polynomial with integer coefficients whose degree is n. Note that $f(x) \equiv 0 \pmod{p}$ is equivalent to $g(x) \equiv 0 \pmod{p}$. Since p is a prime, we either have $x - x_0 \equiv 0 \pmod{p}$ which has one solution modulo p, or $q(x) \equiv 0 \pmod{p}$ which has at most n solutions modulo p by our inductive assumption. It follows that there are at most $n+1$ solutions to $f(x) \equiv 0 \pmod{p}$, as desired. ■

5.5 Existence of primitive roots

Now, we are in a position to characterize which integers have primitive roots.

Theorem 5.11 Every odd prime p has a primitive root.

Proof. As in Theorem 5.7, we write $d_k = \operatorname{ord}_p k$ for $1 \leq k \leq p-1$, and define $D = \max_k\{d_k\}$ so that $D \mid \phi(p) = p-1$. Since $d_k \mid D$, we have $k^D \equiv 1 \pmod{p}$ for each k. It turns out that the congruence $x^D - 1 \equiv 0 \pmod{p}$ has $p-1$ solutions modulo p. By Lagrange's Polynomial Congruence Theorem (Theorem 5.10), we have $D \geq p-1$. Combining with the fact that $D \mid p-1$, we have $D = p-1$, and hence, there exists an integer g of order $D = p-1 = \phi(p)$, thereby giving our desired primitive root. ■

Lemma 5.12 For any odd prime p, there exists a primitive root g such that $p \mid (g^{p-1} - 1)$ and $p^2 \nmid (g^{p-1} - 1)$.

Proof. Let g be an arbitrary primitive root of p. Then $g^{p-1} \equiv 1 \pmod{p}$, namely, $p \mid (g^{p-1} - 1)$. If we also have $p^2 \nmid (g^{p-1} - 1)$, there is nothing to prove. If $p^2 \mid (g^{p-1} - 1)$, namely, $g^{p-1} - 1 \equiv 0 \pmod{p^2}$, then we note that $g_* = p + g$ is also a primitive root of p. Meanwhile,

$$\begin{aligned} g_*^{p-1} - 1 = (p+g)^{p-1} - 1 &= \sum_{r=0}^{p-1} \binom{p-1}{r} p^r g^{p-1-r} - 1 \\ &\equiv g^{p-1} + p(p-1)g^{p-2} - 1 \equiv -pg^{p-2} \not\equiv 0 \pmod{p^2}. \end{aligned}$$

Hence, in this case g_* is the desired primitive root. ■

Theorem 5.13 For any odd prime p, let g be a primitive root as in Lemma 5.12. Then for any positive integer α, g is also a primitive root of p^α. In particular, p^α always has an odd primitive root.

Proof. Since g is a primitive root of p as in Lemma 5.12, we have $\operatorname{ord}_p g = \phi(p) = p-1$ and g is such that

$$g^{p-1} = px + 1$$

with $p \nmid x$. Let $\operatorname{ord}_{p^\alpha} g = d$. Then $g^d \equiv 1 \pmod{p^\alpha}$, and thus $g^d \equiv 1 \pmod{p}$. Hence, $(p-1) \mid d$. On the other hand, $d \mid \phi(p^\alpha) = (p-1)p^{\alpha-1}$. Hence, d is of the form $d = (p-1)p^s$

for some $0 \le s \le \alpha - 1$. Now, recalling that $p \nmid x$, we have, with an application of Theorem 4.11,

$$g^d = g^{(p-1)p^s} = (px+1)^{p^s} = \sum_{r=0}^{p^s} \binom{p^s}{r} (px)^r \equiv 1 + p^{s+1}x \not\equiv 1 \pmod{p^{s+2}}.$$

However, $g^d \equiv 1 \pmod{p^\alpha}$. Hence, $s+2 \ge \alpha + 1$. It follows that the only possibility is $s = \alpha - 1$, implying that $\operatorname{ord}_{p^\alpha} g = d = (p-1)p^{\alpha-1} = \phi(p^\alpha)$, or g is a primitive root of p^α. Finally, we observe that both g and $g + p^\alpha$ are primitive roots of p^α, and they are of different parities, thereby concluding the last part. ■

Theorem 5.14 For any odd prime p and positive integer α, let g be an odd primitive root of p^α. Then g is also a primitive root of $2p^\alpha$.

Proof. Note that g being an odd primitive root of p^α implies that $(g, 2p^\alpha) = 1$. Let $d = \operatorname{ord}_{2p^\alpha} g$ and we have $d \mid \phi(2p^\alpha)$. Then $g^d \equiv 1 \pmod{2p^\alpha}$, and hence, $g^d \equiv 1 \pmod{p^\alpha}$. Since g is a primitive root of p^α, we have $\phi(p^\alpha) = \operatorname{ord}_{p^\alpha} g \mid d$. However, $\phi(2p^\alpha) = \phi(p^\alpha) = (p-1)p^{\alpha-1}$. It follows that $d = \phi(2p^\alpha)$, namely, g is a primitive root of $2p^\alpha$. ■

Theorem 5.15 The positive integer m has a primitive root if and only if m is of the form 1, 2, 4, p^α or $2p^\alpha$ where p is an odd prime and α is a positive integer.

Proof. Note that 1 has a primitive root 1, that 2 has a primitive root 1, and that 4 has a primitive root 3. It remains to show that no other positive integers have primitive roots.

We first exclude ingeters m that can be written as $m = st$ with $s, t \ge 3$ and $(s,t) = 1$. Note that Euler's totient function ϕ is multiplicative, namely, $\phi(m) = \phi(s)\phi(t)$. Also, $\phi(s)$ and $\phi(t)$ are even by recalling Theorem 4.2. Thus, $\frac{\phi(m)}{2}$ is a integer. We prove that for any a with $(a,m) = 1$, $a^{\frac{\phi(m)}{2}} \equiv 1 \pmod{m}$. To see this, we have

$$a^{\frac{\phi(m)}{2}} = \left(a^{\phi(s)}\right)^{\frac{\phi(t)}{2}} \equiv 1^{\frac{\phi(t)}{2}} = 1 \pmod{s},$$

and similarly,

$$a^{\frac{\phi(m)}{2}} \equiv 1 \pmod{t}.$$

Note that $(s,t) = 1$ and $st = m$. By Chinese Remainder Theorem, we have $a^{\frac{\phi(m)}{2}} \equiv 1 \pmod{m}$. Hence, m has no primitive roots.

Finally, we exclude integers of the form 2^α with $\alpha \ge 3$. Note that if a is such that $(a, 2^\alpha) = 1$, then a is odd and we write $a = 2b+1$. We prove that $a^{\frac{\phi(2^\alpha)}{2}} = a^{2^{\alpha-2}} \equiv 1 \pmod{2^\alpha}$ always holds true. To see this, we have, with Theorem 4.11 applied,

$$\begin{aligned} a^{\frac{\phi(2^\alpha)}{2}} = (2b+1)^{2^{\alpha-2}} &= \sum_{r=0}^{2^{\alpha-2}} \binom{2^{\alpha-2}}{r} (2b)^r \\ &\equiv 1 + 2^{\alpha-2}(2b) + (2^{\alpha-2}-1)2^{\alpha-3}(2b)^2 \\ &\equiv 1 + 2^{\alpha-1}(b - b^2) \equiv 1 \pmod{2^\alpha}. \end{aligned}$$

Hence 2^α $(\alpha \ge 3)$ has no primitive roots. ■