by Euler's theorem, because $\varphi(49) = 42 = 7\cdot 6$. Since $3^7 \equiv 3 \bmod 7$ and $5^7 \equiv 5 \bmod 7$, by Fermat's little theorem, we conclude that 3^7 and 5^7 are the two exceptions:

$$3^7 \equiv 31 \bmod 49 \quad \text{and} \quad 5^7 \equiv 19 \bmod 49.$$

Hence, the set G_2 of primitive roots modulo $49 = 7^2$ is the union of

$$\{3 + 7k : 0 \leq k \leq 6, k \neq 4\} \quad \text{and} \quad \{5 + 7j : 0 \leq j \leq 6, j \neq 2\}.$$

Alternatively, in the notation of Corollary 8.5.5, we have $H_2 = \{19, 31 \bmod 49\}$, so

$$G_2 = \{a \bmod p^2 : a \equiv 3 \text{ or } 5 \bmod 7, \text{ and } a \not\equiv 19 \text{ or } 31 \bmod 49\}.$$

Finally, for each $k \geq 2$, the set G_k of primitive roots modulo 7^k are those elements that reduce to one of the elements in G_2 modulo 49.

Theorem 8.5.7. *Let $m = 2$, 4, p^k, or $2p^k$, for some odd prime p and some $k \geq 1$. Then, m has a primitive root.*

Proof. If $m = 2$, then $g \equiv 1 \bmod 2$ is a primitive root. If $m = 4$, then $g \equiv 3 \bmod 4$ is one. If p is an odd prime, then there exists a primitive root modulo p by Theorem 8.4.1. Corollary 8.5.5 shows that there is a primitive root modulo p^k for every $k \geq 1$.

It remains to show that $m = 2p^k$ has a primitive root. Let $g \in \mathbb{Z}$ be a primitive root modulo p^k. We distinguish two cases:

- If g is odd, then every power of g is odd, so $g^j \equiv 1 \bmod 2$ for all $j \geq 1$. Thus, $g^j \equiv 1 \bmod 2p^k$ if and only if $g^j \equiv 1 \bmod p^k$. Hence, the multiplicative order of $g \bmod 2p^k$ is the same as the order of $g \bmod p^k$ which is $\varphi(p^k) = \varphi(2p^k)$. Hence, g is also a primitive root modulo $2p^k$.
- If g is even, then g is not even a unit in $\mathbb{Z}/2p^k\mathbb{Z}$ so it cannot be a primitive root. Let $g' = g + p^k$. Then g' is odd, and $g' \equiv g \bmod p^k$, so it is a primitive root modulo p^k. Hence, by our previous bullet point, g' is a primitive root modulo $2p^k$.

Thus, in all cases, $m = 2p^k$ has a primitive root, as we claimed. □

Example 8.5.8. Let $p = 7$. In Example 8.5.4 we showed that 3 is a primitive root modulo 7^k, for all $k \geq 1$. Since $g = 3$ is odd, it follows that 3 is also a primitive root modulo $2 \cdot 7^k$, for all $k \geq 1$.

Similarly, Example 8.5.6 shows that $g = 10$ is a primitive root modulo 7^k, for all $k \geq 1$. However, 10 is even, so it is not a unit modulo $2 \cdot 7^k$. However, $10 + 7^k$ is a primitive root modulo $2 \cdot 7^k$, for all $k \geq 1$. For instance, this shows that 59 is a primitive root modulo 98.

The converse of Theorem 8.5.7 is also true; i.e., if $m \geq 2$ has a primitive root, then $m = 2$, 4, p^k, or $2p^k$ for some odd prime p. Before we prove this fact, we will introduce the concept of indices, which is an analogue of the concept of logarithm.

8.6. Indices

The logarithm in base b, denoted by $\log_b(x)$, is the inverse function of exponentiation in base b, i.e., b^x. Logarithms are quite useful when solving equations where the unknown is in the exponent. Let us see two examples.

Example 8.6.1. Let us find x such that $x^5 = 16807$, using logarithms. Let us take logarithms (in base e, the natural logarithm) on both sides of the equation:

$$5\log x = \log(x^5) = \log(16807).$$

Thus, $\log x = \log(16807)/5 = 1.945910149\ldots$. Now we use the inverse function of $\log x$, the exponential e^x, to retrieve x:

$$x = e^{\log x} = e^{1.945910149\ldots} = 7.$$

Example 8.6.2. Let us find x such that $7^{x+3} = 16807$. Notice that $16807 = 7^5$. Let us take logarithms in base 7 of both sides:

$$x+3 = \log_7(7^{x+3}) = \log_7(16807) = \log_7(7^5) = 5.$$

Thus, $x+3=5$, so $x=2$.

Here are the key properties of the exponential and logarithm functions that make them so useful in the applications. Let $b > 1$ be fixed. Then:

(a) b^x is a bijection, from $\mathbb{R}$ to $\mathbb{R}^+$, and $\log_b(x)$ is a bijection, from $\mathbb{R}^+$ to $\mathbb{R}$;
(b) $\log_b(x)$ is the inverse function of b^x;
(c) $\log_b(x^n) = n \cdot \log_b(x)$;
(d) $\log_b(xy) = \log_b(x) + \log_b(y)$;
(e) and (perhaps the most important property of all) we can calculate b^x and $\log_b(x)$ efficiently.

In this section, we want to define an analog of the logarithm function for the units modulo m, i.e., $U_m = (\mathbb{Z}/m\mathbb{Z})^\times$. Clearly, if g is a primitive root, then g^x is a bijection;

$$g^x\colon \{1,2,\ldots,\varphi(m)\} \to U_m.$$

Thus, we can define a "logarithm in base g" (an *index* function for the powers of g) as the inverse function of g^x. This is exactly what we will do, and we will show that our index function satisfies properties (a) through (e) above. The following is a *preliminary* definition of the concept of index, which we will refine below in Definition 8.6.7.

Definition 8.6.3. Let $m \geq 2$ be an integer, such that there exists a primitive root g modulo m. We define the *index function* in base g as the function

$$\mathrm{ind}_g\colon (\mathbb{Z}/m\mathbb{Z})^\times \to \{1,2,\ldots,\varphi(m)\}$$

such that $n = \mathrm{ind}_g(a \bmod m)$ is the smallest integer $n \geq 1$ with $g^n \equiv a \bmod m$.

Example 8.6.4. In Example 8.2.2 we showed that $g=2$ is a primitive root modulo 11. We indeed calculated a table of powers of 2 mod 11:

x mod 11	x^2	x^3	x^4	x^5	x^6	x^7	x^8	x^9	x^{10}
2	4	8	5	10	9	7	3	6	1

Using this table, we can calculate values of ind_2, the index in base 2. For instance, $\mathrm{ind}_2(9) = 6$, because $2^9 \equiv 6 \bmod 11$. Similarly, $\mathrm{ind}_2(3) = 8$ because $2^8 \equiv 3 \bmod 11$. We can also build a table of all indices in base 2:

a mod 11	1	2	3	4	5	6	7	8	9	10
$\mathrm{ind}_2(a)$	10	1	8	2	4	9	7	3	6	5

Example 8.6.5. In Example 8.2.8, we showed that $g \equiv 3 \bmod 43$ is a primitive root in $\mathbb{Z}/43\mathbb{Z}$. Let us calculate a table of indices in base 3. First, let us calculate a table of powers of 3 modulo 43:

$x \bmod 43$	x^2	x^3	x^4	x^5	x^6	x^7	x^8	x^9	x^{10}	x^{11}	x^{12}	x^{13}
3	9	27	38	28	41	37	25	32	10	30	4	12
	x^{14}	x^{15}	x^{16}	x^{17}	x^{18}	x^{19}	x^{20}	x^{21}	x^{22}	x^{23}	x^{24}	x^{25}
	36	22	23	26	35	19	14	42	40	34	16	5
	x^{26}	x^{27}	x^{28}	x^{29}	x^{30}	x^{31}	x^{32}	x^{33}	x^{34}	x^{35}	x^{36}	x^{37}
	15	2	6	18	11	33	13	39	31	7	21	20
	x^{38}	x^{39}	x^{40}	x^{41}	x^{42}							
	17	8	24	29	1							

And now we can calculate a table of indices in base 3:

$a \bmod 43$	1	2	3	4	5	6	7	8	9	10	11	12	13	14
$\mathrm{ind}_3(a)$	42	27	1	12	25	28	35	39	2	10	30	13	32	20
$a \bmod 43$	15	16	17	18	19	20	21	22	23	24	25	26	27	28
$\mathrm{ind}_3(a)$	26	24	38	29	19	37	36	15	16	40	8	17	3	5
$a \bmod 43$	29	30	31	32	33	34	35	36	37	38	39	40	41	42
$\mathrm{ind}_3(a)$	41	11	34	9	31	23	18	14	7	4	33	22	6	21

Remark 8.6.6. Let m be a positive integer and suppose that $\gcd(a, m) = 1$. Then, $a^s \equiv a^t \bmod m$ if and only if $s \equiv t \bmod (\mathrm{ord}_m(a))$. Indeed, if $a^s \equiv a^t \bmod m$, then $a^{s-t} \equiv 1 \bmod m$, and $\mathrm{ord}_m(a)$ must be a divisor of $s - t$ (by Proposition 8.1.5). Hence $s \equiv t \bmod (\mathrm{ord}_m(a))$.

Conversely, if $s \equiv t \bmod (\mathrm{ord}_m(a))$, then $s - t = n \cdot \mathrm{ord}_m(a)$ and

$$a^{s-t} \equiv (a^{\mathrm{ord}_m(a)})^n \equiv 1^n \equiv 1 \bmod m,$$

and, therefore, $a^s \equiv a^t \bmod m$.

In particular, if g is a primitive root modulo m and $g^s \equiv b \bmod m$, then $g^t \equiv b \bmod m$, for all $t \equiv s \bmod \varphi(m)$, because $\mathrm{ord}_m(g) = \varphi(m)$. This means that $\mathrm{ind}_g(b)$ can be regarded as the congruence class of $s \bmod \varphi(m)$.

In light of Remark 8.6.6, we redefine the index function as follows.

Definition 8.6.7. Let $m \geq 2$ be an integer, such that there exists a primitive root g modulo m. We define the *index function* in base g as the function

$$\mathrm{ind}_g \colon (\mathbb{Z}/m\mathbb{Z})^\times \to \mathbb{Z}/\varphi(m)\mathbb{Z}$$

such that $n \equiv \mathrm{ind}_g(a \bmod m) \bmod \varphi(m)$ is in the unique congruence class modulo $\varphi(m)$ that satisfies $g^n \equiv a \bmod m$.

With this definition, we are ready to show that the index function satisfies properties very similar to the logarithm.

Proposition 8.6.8. *Let $m \geq 2$ be an integer such that there exists a primitive root g modulo m. Then, the function ind_g satisfies the following properties:*

(a) *g^x is a bijection, from $\mathbb{Z}/\varphi(m)\mathbb{Z}$ to $U_m = (\mathbb{Z}/m\mathbb{Z})^\times$, and ind_g is a bijection, from U_m to $\mathbb{Z}/\varphi(m)\mathbb{Z}$.*

(b) *$\operatorname{ind}_g(x)$ is the inverse function of g^x.*

(c) *$\operatorname{ind}_g(x^t) \equiv t \cdot \operatorname{ind}_g(x) \bmod \varphi(m)$.*

(d) *$\operatorname{ind}_g(xy) \equiv \operatorname{ind}_g(x) + \operatorname{ind}_g(y) \bmod \varphi(m)$.*

Proof. Since g is a primitive root, the map g^x is surjective on $(\mathbb{Z}/m\mathbb{Z})^\times$. By Remark 8.6.6, $g^x \equiv g^y \bmod m$ if and only if $x \equiv y \bmod \varphi(m)$. Thus, g^x is injective with domain $\mathbb{Z}/\varphi(m)\mathbb{Z}$. Hence, g^x is a bijection. The index function ind_g is defined to be the inverse function of g^x, so it is also a bijection. This shows (a) and (b).

Let $n \equiv \operatorname{ind}_g(x \bmod m)$. Then, n is in the unique congruence class modulo $\varphi(m)$ that satisfies $g^n \equiv x \bmod m$. It follows that $g^{tn} \equiv x^t \bmod m$, and so $\operatorname{ind}_g(x^t) \equiv t \cdot n \equiv t \cdot \operatorname{ind}_g(x) \bmod \varphi(m)$. This is (c).

Let $u \equiv \operatorname{ind}_g(x \bmod m)$ and $v \equiv \operatorname{ind}_g(y \bmod m) \bmod \varphi(m)$. Then, $g^u \equiv x$ and $g^v \equiv y \bmod m$. Hence,

$$g^{u+v} \equiv g^u \cdot g^v \equiv x \cdot y \bmod m.$$

This implies that

$$\operatorname{ind}_g(x) + \operatorname{ind}_g(y) \equiv u + v \equiv \operatorname{ind}_g(xy) \bmod \varphi(m),$$

as claimed in (d). □

Remark 8.6.9. Note that property (d) in Proposition 8.6.8 would not be true if the index function was integer-valued (as we had preliminarily defined it in Definition 8.6.3) instead of $\mathbb{Z}/\varphi(m)\mathbb{Z}$-valued.

Traditional exponentials and logarithms can be calculated efficiently (any calculator can do that!). In order to use indices, however, (i) there must be a primitive root modulo m, (ii) we need to be able to find an explicit primitive root g modulo m, and (iii) we need a table of indices in base g.

Example 8.6.10. Let us find all the solutions to the congruence $3x^6 \equiv 4 \bmod 11$, using indices. In Example 8.6.4 we calculated a table of indices in base 2:

$a \bmod 11$	1	2	3	4	5	6	7	8	9	10
$\operatorname{ind}_2(a)$	10	1	8	2	4	9	7	3	6	5

Taking indices on both sides of $3x^6 \equiv 4 \bmod 11$ and using the properties of Proposition 8.6.8, we obtain on one hand $\operatorname{ind}_2(4) \equiv 2 \bmod 10$ and on the other hand

$$2 \equiv \operatorname{ind}_2(4) \equiv \operatorname{ind}_2(3x^6) \equiv \operatorname{ind}_2(3) + \operatorname{ind}_2(x^6) \equiv 8 + 6\operatorname{ind}_2(x) \bmod 10.$$

Therefore, $6\operatorname{ind}_2(x) \equiv 2 - 8 \equiv -6 \equiv 4 \bmod 10$. Solving the congruence $6t \equiv 4 \bmod 10$ is equivalent to finding the solutions of $10s + 6t = 4$, which in turn is equivalent to finding solutions to the diophantine equation $5s + 3t = 2$. Using what we learned in Section 2.9, we find the solution to be

$$s = 1 + 3k,\ t = -1 - 5k$$

for each $k \in \mathbb{Z}$. Hence, $t \equiv -1 \equiv 4 \bmod 5$, which means $t \equiv 4$ or $9 \bmod 10$. It follows that the solutions x to our original equation satisfy

$$\mathrm{ind}_2(x) \equiv 4 \quad \text{or} \quad 9 \bmod 10$$

and by our table, these indices correspond to $x \equiv 5$ or $6 \bmod 11$. Indeed,

$$3 \cdot 5^6 \equiv 46875 \equiv 4 \bmod 11$$

and since $6 \equiv -5 \bmod 11$, it follows that $3 \cdot 6^6 \equiv 3 \cdot (-5)^6 \equiv 3 \cdot 5^6 \equiv 4 \bmod 11$.

In general, there is a formula for the number of solutions of $x^k \equiv a \bmod m$, which is given in the following theorem, and it is an application of indices.

Theorem 8.6.11. *Let $m \geq 2$ and suppose that $\mathbb{Z}/m\mathbb{Z}$ has a primitive root. Let $\gcd(a, m) = 1$. Then, the congruence $x^k \equiv a \bmod m$ has a solution if and only if*

$$a^{\varphi(m)/\gcd(k,\varphi(m))} \equiv 1 \bmod m.$$

If $x^k \equiv a \bmod m$ is solvable, then it has exactly $\gcd(k, \varphi(m))$ different solutions in $\mathbb{Z}/m\mathbb{Z}$.

Proof. Let g be a primitive root modulo m. Then, the congruence $x^k \equiv a \bmod m$ has a solution $x \bmod m$ if and only if $k \cdot \mathrm{ind}_g(x) \equiv \mathrm{ind}_g(a) \bmod \varphi(m)$. Moreover, by Theorem 4.4.3, the congruence $ky \equiv b \bmod \varphi(m)$ has a solution $y_0 \bmod m$ if and only if $d = \gcd(k, \varphi(m))$ is a divisor of b, and if it has a solution, then it has exactly d different solutions modulo $\varphi(m)$. We need a lemma to finish our proof.

Lemma 8.6.12. *Let $m \geq 2$ and suppose that $\mathbb{Z}/m\mathbb{Z}$ has a primitive root. Let $\gcd(a, m) = 1$ and let d be a divisor of $\varphi(m)$. Then, $\mathrm{ind}_g(a) \equiv 0 \bmod d$ if and only if $a^{\varphi(m)/d} \equiv 1 \bmod m$ if and only if $\mathrm{ord}_m(a)$ is a divisor of $\varphi(m)/d$.*

Proof. Suppose that $a^{\varphi(m)/d} \equiv 1 \bmod m$. Taking indices in base g we obtain an equivalent expression

$$(\varphi(m)/d) \cdot \mathrm{ind}_g(a) \equiv \mathrm{ind}_g(1) \equiv 0 \bmod \varphi(m),$$

which is equivalent to $\mathrm{ind}_g(a) \equiv 0 \bmod d$ by Proposition 4.3.1. This concludes the proof of the lemma. $\square$

Back to the proof of Theorem 8.6.11, $a^{\varphi(m)/d} \equiv 1 \bmod m$ if and only if $\mathrm{ind}_g(a) \equiv 0 \bmod d$ if and only if $k \cdot \mathrm{ind}_g(x) \equiv \mathrm{ind}_g(a) \bmod \varphi(m)$ has d solutions for $\mathrm{ind}_g(x)$ and these correspond to d different solutions of $x^k \equiv a \bmod m$. $\square$

Example 8.6.13. In Example 8.6.10 we saw that the congruence $3x^6 \equiv 4 \bmod 11$ has two solutions, namely $x \equiv 5, 6 \bmod 11$. Let us show that there are two solutions using Theorem 8.6.11. The congruence in question is equivalent to

$$x^6 \equiv 4 \cdot 3^{-1} \equiv 4 \cdot 4 \equiv 16 \equiv 5 \bmod 11.$$

Hence, Theorem 8.6.11 says that there are $\gcd(6, 10) = 2$ solutions if $5^{10/2} = 5^5 \equiv 1 \bmod 11$. So it only remains to calculate

$$5^5 \equiv 5 \cdot (5^2)^2 \equiv 5 \cdot (25)^2 \equiv 5 \cdot 3^2 \equiv 5 \cdot 9 \equiv 5 \cdot (-2) \equiv -10 \equiv 1 \bmod 11.$$

Next, we list a few corollaries of Theorem 8.6.11. If $m = p$ is prime, then we know the existence of a primitive root modulo p (by Theorem 8.4.1).

Corollary 8.6.14. *Let p be a prime and let $\gcd(a,p)=1$. Then, a is congruent to a kth power in $\mathbb{Z}/p\mathbb{Z}$ if and only if*

$$a^{(p-1)/\gcd(k,p-1)} \equiv 1 \bmod p.$$

Corollary 8.6.15. *Suppose that there exists a primitive root modulo m. Then:*

(1) *The congruence $x^k \equiv 1 \bmod m$ has exactly $\gcd(k,\varphi(m))$ distinct solutions in $\mathbb{Z}/m\mathbb{Z}$. In particular, if k is a divisor of $\varphi(m)$, then $x^k \equiv 1 \bmod m$ has exactly k solutions.*

(2) *The number of distinct kth powers modulo m is $\varphi(m)/\gcd(k,\varphi(m))$.*

Proof. Part (1) follows directly from Theorem 8.6.11, with $a=1$. For part (2), we note that b is a kth power if and only if $b^{\varphi(m)/\gcd(k,\varphi(m))} \equiv 1 \bmod m$ if and only if b is a solution of $x^{\varphi(m)/\gcd(k,\varphi(m))} \equiv 1 \bmod m$. By part (1), the latter congruence has exactly $\varphi(m)/\gcd(k,\varphi(m))$ solutions. $\square$

Example 8.6.16. The congruences $x^6 \equiv 1$ and $x^7 \equiv 1 \bmod 43$ have, respectively, 6 solutions and 7 solutions, but $x^5 \equiv 1 \bmod 43$ only has one solution ($x \equiv 1 \bmod 43$), because $\gcd(6,\varphi(43))=6$, $\gcd(7,42)=7$, but $\gcd(5,42)=1$. Let us calculate the solutions to each of these congruences using indices. Recall that in Example 8.6.5 we have calculated a table of indices in base 3:

$a \bmod 43$	1	2	3	4	5	6	7	8	9	10	11	12	13	14
$\mathrm{ind}_3(a)$	42	27	1	12	25	28	35	39	2	10	30	13	32	20
$a \bmod 43$	15	16	17	18	19	20	21	22	23	24	25	26	27	28
$\mathrm{ind}_3(a)$	26	24	38	29	19	37	36	15	16	40	8	17	3	5
$a \bmod 43$	29	30	31	32	33	34	35	36	37	38	39	40	41	42
$\mathrm{ind}_3(a)$	41	11	34	9	31	23	18	14	7	4	33	22	6	21

Now, taking indices on the congruence $x^6 \equiv 1 \bmod 43$ we obtain

$$6\,\mathrm{ind}_3(x) \equiv \mathrm{ind}_3(1) \equiv 42 \equiv 0 \bmod 42,$$

and therefore $\mathrm{ind}_3(x) \equiv 0 \bmod 7$, so that $\mathrm{ind}_3(x) \equiv 7k \bmod 42$, for $0 \le k \le 5$. In other words, $\mathrm{ind}_3(x) \equiv 0,7,14,21,28,35 \bmod 42$, and these correspond to

$$x \equiv 1,37,36,42,6,7 \bmod 43,$$

respectively. Notice that to find x knowing $\mathrm{ind}_3(x)$, it is best to use the table of powers of 3 (as it appears in Example 8.6.5). Similarly, $x^7 \equiv 1 \bmod 43$ is equivalent to $7\,\mathrm{ind}_3(x) \equiv 0 \bmod 42$, which means that $\mathrm{ind}_3(x) \equiv 0 \bmod 6$, and the solutions satisfy $\mathrm{ind}_3(x) \equiv 6j \bmod 42$ for $0 \le j \le 6$. These correspond to

$$x \equiv 1,41,4,35,16,11,21 \bmod 43.$$

Last, $x^5 \equiv 1 \bmod 43$ translates to $5\,\mathrm{ind}_3(x) \equiv 0 \bmod 42$. Since $\gcd(5,42)=1$, this means that $\mathrm{ind}_3(x) \equiv 0 \bmod 42$, and there is a unique solution; namely, $x \equiv 1 \bmod 43$.