# 3 Primitive Roots, Indices and the Discrete Logarithm

It is well-understood that exponential and logarithmic functions are mutual inverses when thought of as functions on the real numbers:

$$y = g^x \iff x = \log_g y$$

This is number theory, so we want to know if something similar can be said for integers, or more precisely within modular arithmetic. The first operation, taking powers, makes perfect sense: for instance $5^3 \equiv 8 \pmod 9$. To what extent can we reverse this? In our example, is it reasonable to write, and/or make sense of, the following?

$$3 \equiv \log_5 8 \pmod 9$$

Answering this question will lead to the notion of a *discrete logarithm.*

## 3.1 A Little Abstract Algebra: Groups, Rings and Units

We start with a primer on group/ring theory.

**Definition 3.1.** A *group* is a set $G$ together with a binary operation $\cdot$ which satisfies the following properties:

- *Closure*: $\forall x, y \in G$, we have $x \cdot y \in G$.
- *Associativity*: $\forall x, y, z \in G$, we have $(x \cdot y) \cdot z = x \cdot (y \cdot z)$.
- *Identity*: $\exists e \in G$ such that $\forall x \in G$ we have $e \cdot g = g \cdot e = g$.
- *Inverse*: $\forall x \in G$, $\exists y \in G$ such that $x \cdot y = y \cdot x = e$.

A group is *abelian* if $\cdot$ is *commutative*: that is if $\forall x, y \in G$ we have $x \cdot y = y \cdot x$.
A *ring* is a set $R$ together with two binary operations $+$ and $\cdot$, which satisfy the following:

- $R$ is an abelian group under $+$: the symbol 0 is often used for the additive identity element, i.e. $\forall x \in R,\ 0 + x = x + 0 = x$.
- $R$ is associative with respect to $\cdot$.
- $R$ has a multiplicative identity element, often called 1: i.e. $\forall x \in R,\ 1 \cdot x = x \cdot 1 = x$.
- $R$ has the *distributive laws*: $\forall x, y, z \in R$, we have

$$x \cdot (y + z) = x \cdot y + x \cdot z, \qquad (x + y) \cdot z = x \cdot z + y \cdot z$$

A ring is a *field* $F$ if multiplication is commutative and every non-zero element has a multiplicative inverse: otherwise said, we require $F \setminus \{0\}$ to be an abelian group under multiplication.

Rings generalize the concepts of addition and multiplication, while a field also does this for division by non-zero elements. In number theory, the prototypical examples of rings are the sets of remainders $\mathbb{Z}_n$ under addition and multiplication modulo $n$, although we shall see others later. It is worth recalling the following related results, and how they can be rephrased in terms of groups and rings:

**Theorem 3.2.** *1. (*Bézout's identity*)* $\gcd(g,n) = 1 \iff \exists h, s \in \mathbb{Z}$ *such that* $gh + ns = 1$.

*2. (*Division in $\mathbb{Z}_n$*)* $gx \equiv gy \pmod{n} \implies x \equiv y \ (\mathrm{mod}\ \frac{)}{n}\gcd(g,n)$.

The first part of the Theorem can instead be written:

$$\begin{aligned}\gcd(g,n) = 1 &\iff \exists h \in \mathbb{Z} \text{ such that } gh \equiv 1 \pmod{n}\\ &\iff \exists h \in \mathbb{Z}_n \text{ such that } gh = 1\\ &\iff g \text{ has a multiplicative inverse } h = g^{-1} \text{ in } \mathbb{Z}_n\end{aligned}$$

We have the following immediate consequences:

**Corollary 3.3.** *1. The set of remainders coprime to* $n$ *is an* abelian group under multiplication.

*2.* $\mathbb{Z}_n$ *is a field if and only if* $n$ *is prime.*

**Definition 3.4.** The set $\mathbb{Z}_n^\times := \{x \in \mathbb{Z}_n : \gcd(x,n) = 1\}$ is the group[a] of *units* modulo $n$.

[a] Generally, a unit is an element with has a multiplicative inverse: the set of such forms a group under multiplication.

Recall that the number of units modulo $n$ is given by Euler's totient function $\varphi(n)$.

**Example 3.5.** In $\mathbb{Z}_4$, the addition and multiplication tables are

| $+_4$ | 0 | 1 | 2 | 3 |
|---|---|---|---|---|
| 0 | 0 | 1 | 2 | 3 |
| 1 | 1 | 2 | 3 | 0 |
| 2 | 2 | 3 | 0 | 1 |
| 3 | 3 | 0 | 1 | 2 |

| $\cdot_4$ | 0 | 1 | 2 | 3 |
|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | 2 | 3 |
| 2 | 0 | 2 | 0 | 2 |
| 3 | 0 | 3 | 2 | 1 |

One can see the group of units in the second table:

$\mathbb{Z}_4^\times = \{1, 3\}$

| $\cdot_4$ | 1 | 3 |
|---|---|---|
| 1 | 1 | 3 |
| 3 | 3 | 1 |

Modulo 10, we have $\mathbb{Z}_{10}^\times = \{1, 3, 7, 9\}$ and, with a slight rearrangement, the multiplication table

| $\cdot_{10}$ | 1 | 3 | 9 | 7 |
|---|---|---|---|---|
| 1 | 1 | 3 | 9 | 7 |
| 3 | 3 | 9 | 7 | 1 |
| 9 | 9 | 7 | 1 | 3 |
| 7 | 7 | 1 | 3 | 9 |

Up to relabelling, this has exactly the same form as that for $\mathbb{Z}_4$ under addition. We say that the groups $(\mathbb{Z}_{10}^\times, \cdot_{10})$ and $(\mathbb{Z}_4, +_4)$ are *isomorphic* and that the function

$$\mu : \mathbb{Z}_{10}^\times \to \mathbb{Z}_4 : (1, 3, 9, 7) \mapsto (0, 1, 2, 3)$$

is an *isomorphism.*

**Definition 3.6.** Groups $G$ and $H$ are *isomorphic* if there exists a function $\mu : G \to H$ which satisfies:

1. $\mu$ is bijective;
2. $\mu$ is a *homomorphism*: $\forall g_1, g_2 \in G$, we have $\mu(g_1 \cdot_G g_2) = \mu(g_1) \cdot_H \mu(g_2)$.

We call $\mu$ an *isomorphism* and write $G \cong H$.

The above groups have another special property.

**Definition 3.7.** The *cyclic subgroup generated by* $g \in G$ is the set[a]

$$\langle g \rangle = \{g^k : k \in \mathbb{Z}\} = \{\ldots, g^{-1}, e, g, g^2, \ldots\}$$

A group $G$ is *cyclic* if there exists $g$ such that $G = \langle g \rangle$: we call $g$ a *generator* of $G$.

[a] It is conventional to take $g^0 = e$ (the identity) and $g^k = (g^{-1})^k$ if $k < 0$. Our definition is for groups where the operation is multiplication: in an additive group, $x = \underbrace{g + \cdots + g}_{k \text{ times}} = kg$.

**Example (3.5, mk. II).** $(\mathbb{Z}_4, +)$ is generated by 1, since

$$\langle 1 \rangle = \{1, 1+1, 1+1+1, 1+1+1+1, \ldots\} = \{1, 2, 3, 0\} = \mathbb{Z}_4$$

$(\mathbb{Z}_{10}^\times, \cdot)$ is generated by 3, since

$$\langle 3 \rangle = \{3, 3^2, 3^3, 3^4, \ldots\} = \{3, 9, 7, 1\} = \mathbb{Z}_{10}^\times$$

Both groups are cyclic, and the isomorphism $\mu$ maps a generator of $\mathbb{Z}_{10}^\times$ to a generator of $\mathbb{Z}_4$. In fact the generator approach allows us to spot a simple formula for the isomorphism:

$$\mu(3^x) = x$$

Otherwise said, $\mu$ is playing the role of $\log_3$.

It is worth thinking a little about the standard (continuous) logarithms in this language. If $b > 0$ and $b \neq 1$, then the logarithm base $b$ is a bijection

$$\log_b : \mathbb{R}^+ \to \mathbb{R} \quad \text{such that} \quad \log_b(xy) = \log_b(x) + \log_b(y)$$

Otherwise said, $\log_b : (\mathbb{R}^+, \cdot) \to (\mathbb{R}, +)$ is a *group isomorphism*. This motivates our search for discrete logartihms: such should be isomorphisms of groups $\mu : (\mathbb{Z}_n^\times, \cdot) \to (\mathbb{Z}_{\varphi(n)}, +)$.

**Exercises**

1. We work in the ring $\mathbb{Z}_7$ of remainders modulo 7.
   (a) Compute the values $3^x$ in $\mathbb{Z}_7$, show that the group of units $\mathbb{Z}_7^\times$ is cyclic and describe an isomorphism $\mu : \mathbb{Z}_7^\times \to \mathbb{Z}_6$.
   (b) Use your answer to part (a) to solve the equation $3^x \equiv 6 \pmod 7$.
2. Find the group of units $\mathbb{Z}_8^\times$ modulo 8 and show that it is *not* cyclic.
3. If $x$ and $y$ are units, prove directly that $xy$ is also a unit.

### 3.2 Primitive Roots

We have the following questions:

- Is it always possible to define a logarithm-like function $\mu : \mathbb{Z}_n^\times \to \mathbb{Z}_{\varphi(n)}$ as we did above? More precisely, for which moduli $n$ can this be done?
- Given $n$, for what bases (e.g. $g = 3$ modulo 10 in the above example) can this be done?

To start answering these questions, we need a new piece of terminology.

**Definition 3.8.** If $g \in \mathbb{Z}_n^\times$, define the *order of $g$* modulo $n$ to be

$$e_n(g) = \min\{k \in \mathbb{N} : g^k \equiv 1 \pmod{n}\}$$

More generally, the order of a group $G$ is its cardinality: the order of an element $g \in G$ is the order of the cyclic subgroup $\langle g \rangle$. Indeed it should be easy to convince yourself that

$$\langle g \rangle = \{g, g^2, g^3, \ldots\} = \{g, g^2, \ldots, g^{e_n(g)-1}, 1\}$$

since $g^{e_n(g)} \equiv 1 \pmod{n}$. The following proof should help if you're stuck...

**Theorem 3.9.** *The order of an element $g \in \mathbb{Z}_n^\times$ divides $\varphi(n)$.*

This is just an special case of Lagrange's Theorem from Group Theory: the order of an element divides the order of the group. Here is a proof adapted to our situation.

*Proof.* We know that $g^{e_n(g)} \equiv 1 \pmod{n}$. Now assume that $g^k \equiv 1 \pmod{n}$ where $k > 0$. By the division algorithm, we know that there exist unique $q, r \in \mathbb{N}$ such that

$$\begin{cases} k = q\, e_n(g) + r \\ 0 \le r < e_n(g) \end{cases}$$

It follows that

$$1 \equiv g^k \equiv g^{q\, e_n(g)+r} \equiv (g^{e_n(g)})^q \cdot g^r \equiv g^r \pmod{n}$$

This is a contradiction unless $r = 0$, since $e_n(g)$ is the smallest positive power that raises $g$ to obtain 1. It follows that $e_n(g) \mid k$.
Finally, Euler's Theorem says that $g^{\varphi(n)} \equiv 1 \pmod{n}$: taking $k = \varphi(n)$ gives the result. ■

Our notion of a discrete logarithm is predicated on the existence of an isomorphism between $\mathbb{Z}_n^\times$ and $\mathbb{Z}_{\varphi(n)}$. Otherwise said, *we want $\mathbb{Z}_n^\times$ to be cyclic.* Since a cyclic group requires a generator...

**Definition 3.10.** A unit $g \in \mathbb{Z}_n^\times$ is a *primitive root modulo $n$* if $e_n(g) = \varphi(n)$.
Equivalently, $g$ is a generator of the group of units: $\langle g \rangle = \mathbb{Z}_n^\times$.

In the special case that $n = p$ is prime, recall that $\varphi(p) = p - 1$ since every non-zero element of $\mathbb{Z}_p$ is a unit. An element $g \in \mathbb{Z}_p^\times$ is therefore a primitive root provided $e_p(g) = p - 1$.

**Examples 3.11.** 1. Thinking back to page 2 we see that 3 is the only primitive root modulo 4: since $3^2 \equiv 1 \pmod 4$, the subgroup of $\mathbb{Z}_4^\times$ generated by 3 is $\langle 3 \rangle = \{3, 1\} = \mathbb{Z}_4^\times$.

2. Also from the same page, we see that the primitive roots modulo 10 are 3 and 7. Written in order $g^1, g^2, g^3, \ldots$, the subgroups generated by the primitive roots are

$$\langle 3 \rangle = \{3, 9, 7, 1\}, \qquad \langle 7 \rangle = \{7, 9, 3, 1\}$$

Note that $\langle 9 \rangle = \{9, 1\}$ since $9^2 \equiv 1 \,(\text{mod } 10)$, thus 9 is not a primitive root modulo 10.

3. Here is the multiplication table for $\mathbb{Z}_{14}^\times = \{1, 3, 5, 9, 11, 13\}$ in its full glory:

| $\cdot_{14}$ | 1 | 3 | 5 | 9 | 11 | 13 |
|---|---|---|---|---|---|---|
| 1 | 1 | 3 | 5 | 9 | 11 | 13 |
| 3 | 3 | 9 | 1 | 13 | 5 | 11 |
| 5 | 5 | 1 | 11 | 3 | 13 | 9 |
| 9 | 9 | 13 | 3 | 11 | 1 | 5 |
| 11 | 11 | 5 | 13 | 1 | 9 | 3 |
| 13 | 13 | 11 | 9 | 5 | 3 | 1 |

In this case 3 and 5 are primitive roots and the group of units is isomorphic to $\mathbb{Z}_6$. For each of these generators, consider the elements $g^k$ as $k$ increases:

$$\langle 3 \rangle = \{3, 9, 13, 11, 5, 1\}, \qquad \langle 5 \rangle = \{5, 11, 13, 9, 3, 1\}$$

By contrast, $\langle 9 \rangle = \{9, 11, 1\}$: clearly $e_{14}(9) = 3 \neq \varphi(14)$ whence 9 is not a primitive root.

We list the units for each modulus $\leq 16$. For each unit $g \in \mathbb{Z}_n^\times$, we give its order $e_n(g)$ and thus discover the generators (primitive roots), *if* there are any.[1]

| $n$ | Units $g \in \mathbb{Z}_n^\times$ | Orders of units $e_n(g)$ | Isomorph | Primitive roots |
|---|---|---|---|---|
| 2 | 1 | 1 | $\mathbb{Z}_1$ | 1 |
| 3 | 1, 2 | 1, 2 | $\mathbb{Z}_2$ | 2 |
| 4 | 1, 3 | 1, 2 | $\mathbb{Z}_2$ | 3 |
| 5 | 1, 2, 3, 4 | 1, 4, 4, 2 | $\mathbb{Z}_4$ | 2, 3 |
| 6 | 1, 5 | 1, 2 | $\mathbb{Z}_2$ | 5 |
| 7 | 1, 2, 3, 4, 5, 6 | 1, 3, 6, 3, 6, 2 | $\mathbb{Z}_6$ | 3, 5 |
| 8 | 1, 3, 5, 7 | 1, 2, 2, 2 | $\mathbb{Z}_2 \times \mathbb{Z}_2$ | |
| 9 | 1, 2, 4, 5, 7, 8 | 1, 6, 3, 6, 3, 2 | $\mathbb{Z}_6$ | 2, 5 |
| 10 | 1, 3, 7, 9 | 1, 4, 4, 2 | $\mathbb{Z}_4$ | 3, 7 |
| 11 | 1, 2, 3, 4, 5, 6, 7, 8, 9, 10 | 1, 10, 5, 5, 5, 10, 10, 10, 5, 2 | $\mathbb{Z}_{10}$ | 2, 6, 7, 8 |
| 12 | 1, 5, 7, 11 | 1, 2, 2, 2 | $\mathbb{Z}_2 \times \mathbb{Z}_2$ | |
| 13 | 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12 | 1, 12, 3, 6, 4, 12, 6, 12, 4, 3, 6, 12, 2 | $\mathbb{Z}_{12}$ | 2, 6, 7, 11 |
| 14 | 1, 3, 5, 9, 11, 13 | 1, 6, 6, 3, 3, 2 | $\mathbb{Z}_6$ | 3, 5 |
| 15 | 1, 2, 4, 7, 8, 11, 13, 14 | 1, 4, 2, 4, 4, 2, 4, 2 | $\mathbb{Z}_2 \times \mathbb{Z}_4$ | |
| 16 | 1, 3, 5, 7, 9, 11, 13, 15 | 1, 4, 4, 2, 2, 4, 4, 2 | $\mathbb{Z}_2 \times \mathbb{Z}_4$ | |

See if you can spot any patterns as to which $n$ have primitive roots. It certainly seems that primes have primitive roots, though this is plainly not the whole story.

[1] The isomorph is the abelian group to which $\mathbb{Z}_n^\times$ is isomorphic. This is only relevant to us when primitive roots exist.

### Indices and Calculation

For the present we consider how primitive roots can help us calculate. We know that $g$ is a primitive root modulo $n$ if $g$ generates the group of units $\mathbb{Z}_n^\times$. Thus

$$\mathbb{Z}_n^\times = \{g, g^2, \ldots, g^{\varphi(n)-1}, g^{\varphi(n)}\}$$

The following is immediate:

$$\forall a \in \mathbb{Z}_n^\times,\ \exists \text{ unique } k \in [1, \varphi(n)] : g^k \equiv a \pmod{n}$$

**Definition 3.12.** We call $k = I_g(a)$ the *index*,[a] or *discrete logarithm*, of $a$ with base $g$ modulo $n$.

[a] If the index is understood, you can simply write $I(a)$ for brevity. Some authors prefer $I_g(1) = 0$ rather than $\varphi(n)$.

**Examples 3.13.** 1. Recall that $g = 3$ is a primitive root modulo 10. The powers of $g$ produces a table of indices:

| $k$ | 1 | 2 | 3 | 4 |
|---|---|---|---|---|
| $3^k$ | 3 | 9 | 7 | 1 |

| $a$ | 1 | 3 | 7 | 9 |
|---|---|---|---|---|
| $I_3(a)$ | 4 | 1 | 3 | 2 |

2. Similarly, 5 is a primitive root modulo 14 and we have

| $k$ | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|
| $5^k$ | 5 | 11 | 13 | 9 | 3 | 1 |

| $a$ | 1 | 3 | 5 | 9 | 11 | 13 |
|---|---|---|---|---|---|---|
| $I_5(a)$ | 6 | 5 | 1 | 4 | 2 | 3 |

3. When $n = 11$, we have $g = 2$ as a primitive root. This time the tables are

| $k$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
|---|---|---|---|---|---|---|---|---|---|---|
| $2^k$ | 2 | 4 | 8 | 5 | 10 | 9 | 7 | 3 | 6 | 1 |

| $a$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
|---|---|---|---|---|---|---|---|---|---|---|
| $I_2(a)$ | 10 | 1 | 8 | 2 | 4 | 9 | 7 | 3 | 6 | 5 |

As an example of a calculation for which indices are helpful, consider

$$5^8 \cdot 7^4 \cdot 8^6 \equiv (2^4)^8 \cdot (2^7)^4 \cdot (2^3)^6 \equiv 2^{78} \equiv 2^8 \equiv 3 \pmod{11}$$

While there are other ways of doing this calculation, it should be clear that the use of indices made things very easy: the problem is that we needed to know the indices first!

You might have heard of *log tables* from the days before calculators: these were large tomes filled with values of logarithms which could be used to simplify large computations. For example, the following procedure was used to multiply large numbers $a$ and $b$:

1. Find $\log_{10} a$ and $\log_{10} b$ in the book of log tables: these will be much smaller than $a$ and $b$.
2. Compute $x = \log_{10} a + \log_{10} b$.
3. By the log laws, $ab = 10^x$, which could be looked up in a log table or otherwise approximated.

Such calculations were very simple, *provided you had access to the log table!* Indices perform the same role for modular exponentiation: if you already have a table of indices and are only computing with units, then calculations are significantly simplified.

Since the exponential laws hold in modular arithmetic, so too do the standard logarithm laws.

**Theorem 3.14.** *If $I(a)$ is the index with respect to a primitive root $g \in \mathbb{Z}_n^\times$, then*

1. $I(ab) \equiv I(a) + I(b) \pmod{\varphi(n)}$
2. $I(a^k) \equiv kI(a) \pmod{\varphi(n)}$

The primary challenge is to remember to reduce indices modulo $\varphi(n)$, *not modulo $n$!*

*Proof.* We prove part 1 similarly to the logarithm laws you'll find in an algebra textbook. Since $a, b$ are units, we know that $g^{I(a)} \equiv a$ and $g^{I(b)} \equiv b \pmod{n}$. Moreover, $ab$ is a unit, so we also have $ab \equiv g^{I(ab)}$. By the law of exponents,

$$g^{I(ab)} \equiv ab \equiv g^{I(a)}g^{I(b)} \equiv g^{I(a)+I(b)} \implies g^{I(ab)-I(a)-I(b)} \equiv 1 \pmod{n}$$

Since $g$ is a primitive root, it follows that $I(ab) \equiv I(a) + I(b) \pmod{\varphi(n)}$. ∎

Here is Example 3.13.3 recast in this language:

$$\begin{aligned} I_2(5^8 \cdot 7^4 \cdot 8^6) &\equiv 8I_2(5) + 4I_2(7) + 6I_2(8) \equiv 8 \cdot 4 + 4 \cdot 7 + 6 \cdot 3 \equiv 8 \equiv I_2(3) \pmod{10} \\ &\implies 5^8 \cdot 7^4 \cdot 8^6 \equiv 3 \pmod{11} \end{aligned}$$

### Solving Equations with Indices

In elementary algebra, we can solve equations using alogarithms: e.g.,

$$\begin{aligned} 5x^3 = 8 &\implies \ln 5 + 3\ln x = \ln 8 \\ &\implies \ln x = \frac{\ln 8 - \ln 5}{3} = \frac{1}{3}\ln\frac{8}{5} = \ln\left(\frac{8}{5}\right)^{1/3} \\ &\implies x = \left(\frac{8}{5}\right)^{1/3} \end{aligned}$$

Indices and primitive roots work the same way for congruence equations. The only problem is that we need to have previously computed a table of indices! This approach is therefore appropriate if you expect to have to solve many similar congruences.

**Examples 3.15.** 1. We solve $5x^3 \equiv 8 \pmod{11}$. Recall that 2 is a primitive root modulo 11 and reference the tables of powers/indices on page 6. Now take indices with base 2:

$$\begin{aligned} I(5) + 3I(x) \equiv I(8) &\implies 3I(x) \equiv I(8) - I(5) \equiv 3 - 4 \equiv 9 \pmod{10} \\ &\implies I(x) \equiv 3 \equiv I(8) \pmod{10} \\ &\implies x \equiv 8 \pmod{11} \end{aligned}$$

Things are very simple in comparison to the method you likely saw for solving this in a previous course (Exercise 3.2.7).

2. Solve $27x^{13} \equiv 47 \pmod{50}$, given the following tables for the primitive root $3 \in \mathbb{Z}_{50}^{\times}$

| $k$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $3^k$ | 3 | 9 | 27 | 31 | 43 | 29 | 37 | 11 | 33 | 49 | 47 | 41 | 23 | 19 | 7 | 21 | 13 | 39 | 17 | 1 |

| $a$ | 1 | 3 | 7 | 9 | 11 | 13 | 17 | 19 | 21 | 23 | 27 | 29 | 31 | 33 | 37 | 39 | 41 | 43 | 47 | 49 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $I_3(a)$ | 20 | 1 | 15 | 2 | 8 | 17 | 19 | 14 | 16 | 13 | 3 | 6 | 4 | 9 | 7 | 18 | 12 | 5 | 11 | 10 |

Since 27 and 47 are units, it should be clear that any solution $x$ is also. Now take indices:

$$\begin{aligned} I(27) + 13I(x) \equiv I(47) &\implies 13I(x) \equiv 11 - 3 \equiv 8 \pmod{20} \\ &\implies I(x) \equiv -3 \cdot 8 \equiv -4 \equiv 16 \equiv I(21) \pmod{20} \\ &\implies x \equiv 21 \pmod{50} \end{aligned}$$

where we used the fact that $-3 \cdot 13 \equiv -39 \equiv 1 \pmod{20}$.

3. If $27x^4 \equiv 47 \pmod{50}$, then

$$\begin{aligned} I(27) + 4I(x) \equiv I(47) &\implies 4I(x) \equiv 11 - 3 \equiv 8 \pmod{20} \\ &\implies I(x) \equiv 2 \pmod{5} \\ &\implies I(x) \equiv 2,\ 7,\ 12,\ 17 \pmod{20} \\ &\implies x \equiv 9,\ 37,\ 41,\ 13 \pmod{50} \end{aligned}$$

4. If $27x^5 \equiv 47 \pmod{50}$, then

$$I(27) + 5I(x) \equiv I(47) \implies 5I(x) \equiv 11 - 3 \equiv 8 \pmod{20}$$

This has no solutions, whence the original congruence has no solutions either.

**Exercises** 1. For each unit $g \in \mathbb{Z}_n^{\times}$, compute its order $e_n(g)$:

(a) $e_9(2)$ (b) $e_{15}(2)$ (c) $e_{16}(3)$ (d) $e_{10}(3)$

2. Let $k$ be a positive integer. If $x^k = u$ is a unit in $\mathbb{Z}_n$, prove that $x$ must also be a unit.
3. If $a$ is relatively prime to both $m$ and $n$, and if $\gcd(m,n) = 1$, find a formula for $e_{mn}(a)$ in terms of $e_m(a)$ and $e_n(a)$. Check your answer for $m = 5,\ n = 9,\ a = 2$.
4. If $a \equiv b^2 \pmod{p}$ is a perfect square and $p$ an odd prime, explain why $a$ isn't a primitive root. (*Hint: use Fermat's Little Theorem*)
5. Prove the second index law: $I(a^k) \equiv kI(a) \pmod{\varphi(n)}$.
6. You are given the table of powers base 2, modulo 37.

| $k$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $2^k$ | 2 | 4 | 8 | 16 | 32 | 27 | 17 | 34 | 31 | 25 | 13 | 26 | 15 | 30 | 23 | 9 | 18 | 36 |

| $k$ | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 | 32 | 33 | 34 | 35 | 36 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $2^k$ | 35 | 33 | 29 | 21 | 5 | 10 | 20 | 3 | 6 | 12 | 24 | 11 | 22 | 7 | 14 | 28 | 19 | 1 |

Use the table to find all solutions, if any, to the following congruences modulo 37:

(a) $12x \equiv 23$ (b) $5x^{23} \equiv 18$ (c) $x^{12} \equiv 11$ (d) $7x^{20} \equiv 34$

7. Recall the method for finding unique $k^{\text{th}}$ roots in a previous course.

   *If* $\gcd(b,n) = 1 = \gcd(k,\varphi(n))$ *then* $x^k \equiv b \pmod{n}$ *has the unique solution* $x \equiv b^u \pmod{n}$, *where* $ku \equiv 1 \pmod{\varphi(n)}$

   (a) Use this, after multiplying through by $5^{-1} \equiv 9 \pmod{11}$, to solve $5x^3 \equiv 8 \pmod{11}$

   (b) Why does the old method fail when applied to $27x^4 \equiv 47$ and $27x^5 \equiv 47 \pmod{50}$?

8. You are given that $g = 2$ is a primitive root modulo 27.

   (a) Construct a table of indices for $g = 2$.

   (b) Use your table of indices to solve the congruence $x^{11} \equiv 20 \pmod{27}$.

   (c) Here is an alternative approach, if slower, approach: if $x^{11} \equiv 20$ has a solution, then it must also solve $x^{11} \equiv 2 \pmod{3}$.

      i. Explain why $x \equiv 2 \pmod{3}$.

      ii. Use this to find the solution(s) to part (b)

   (d) Use indices to solve the congruence $x^{21} \equiv 17 \pmod{27}$.

   (e) Find all integers $n \in \mathbb{Z}_{18}$ for which $x^n \equiv 17 \pmod{27}$ has a solution (since $\varphi(27) = 18$, by Euler's Theorem, these are the only $n$ which matter).

### 3.3 Existence of Primitive Roots and the Structure of the Group of Units

If we know that a primitive root exists, then the whole power of cyclic group theory is at our disposal. In particular, we are able to compute precisely how many elements of $\mathbb{Z}_n^\times$ have a particular order.

**Theorem 3.16.** *Suppose that $g$ is a primitive root modulo $n$.*

1. *The order of $g^k$ is* $e_n(g^k) = \dfrac{\varphi(n)}{\gcd(k,\varphi(n))}$

2. *If $d \mid \varphi(n)$, then there are $\varphi(d)$ elements of $\mathbb{Z}_n^\times$ with order $d$. Indeed $g^k$ has order $d$ if and only if*

$$\gcd(k,\varphi(n)) = \frac{\varphi(n)}{d}$$

Part 1 is a special case of a standard result from the theory of cyclic groups (a proof is in the Exercises), while part 2 is an elementary property of Euler's function.[2] Since a primitive root modulo $n$ must have order $\varphi(n)$, we immediately get the following:

**Corollary 3.17.** *If $\mathbb{Z}_n$ has a primitive root $g$, then it has precisely $\varphi(\varphi(n))$ of them: $g^k$ is a primitive root* $\iff \gcd(k,\varphi(n)) = 1$.

One can verify this using examples from the table on page 5: e.g. $n = 14$ has $\varphi(\varphi(14)) = \varphi(6) = 2$ primitive roots.

[2] If $c \mid m$, then there are $\varphi(\frac{m}{c})$ remainders $a \in \mathbb{Z}_m$ such that $\gcd(a,m) = c$. This is since

$$\gcd(a,m) = c \iff \gcd\left(\frac{a}{c},\frac{m}{c}\right) = 1$$

Let $m = \varphi(n)$ and $d = \frac{\varphi(n)}{c}$ for our purposes.

The main thing missing from our discussion is existence! We will at least do this for prime moduli. In essence, the strategy is to prove the previous theorem *without* assuming that a primitive root exists. That is, we count all the terms in $\mathbb{Z}_p^\times$ which have a particular order.

**Theorem 3.18.** *Let $p$ be prime. For each $d \mid p-1$, the set $\{a \in \mathbb{Z}_p^\times : e_p(a) = d\}$ has cardinality $\varphi(d)$. In particular, $p$ has a primitive root (indeed $\varphi(p-1)$ of them).*

Replacing $p-1$ by $\varphi(m)$ results in a *falsehood* for some composites $m$.

*Proof.* We know that $e_p(a) \mid p-1$ for all $a \in \mathbb{Z}_p^\times$. For each $d \mid p-1$, define

$$\psi(d) = \left|\{a \in \mathbb{Z}_p^\times : e_p(a) = d\}\right|$$

Our goal is to show that $\psi(d) = \varphi(d)$. Start by supposing that $p-1 = nk$ and consider

$$x^{p-1} - 1 = x^{nk} - 1 = (x^n - 1)(x^{n(k-1)} + x^{n(k-2)} + \cdots + x^n + 1)$$

We count the number of roots of various parts of this polynomial:

- (Fermat's Little Theorem) $x^{p-1} - 1 \equiv 0 \pmod{p}$ has *exactly* $p-1$ roots: every $1 \le x \le p-1$.
- (Lagrange's Theorem) $x^n - 1 \equiv 0 \pmod{p}$ has *at most* $n$ solutions.
- $x^{n(k-1)} + x^{n(k-2)} + \cdots + x^n + 1 \equiv 0 \pmod{p}$ has *at most* $n(k-1) = p-1-n$ solutions, again by Lagrange.

It follows that the *at mosts* must be *exactly's*: if $n \mid p-1$, then $x^n \equiv 1 \pmod{p}$ has *exactly* $n$ solutions.

Now count these solutions differently. We clearly have[a]

$$x^n \equiv 1 \pmod{p} \iff e_p(x) \mid n$$

If the divisors of $n$ are $d_1, \ldots, d_r$, then the number of solutions to $x^n \equiv 1 \pmod{p}$ is precisely

$$\psi(d_1) + \cdots + \psi(d_r)$$

By the above discussion, this must equal $n$:

$$\sum_{d \mid n} \psi(d) = n$$

This should look familiar: it's the same formula satisfied by the totient function! A quick induction finishes things off.

The base case $\psi(1) = 1 = \varphi(1)$ is clear. Now fix $n \in \mathbb{N}$ and assume that $\psi(d) = \varphi(d)$ for all $d < n$. We know that

$$n = \sum_{d \mid n} \psi(d) = \sum_{d \mid n} \varphi(d)$$

By cancelling all the terms for $d < n$ we conclude that $\psi(n) = \varphi(n)$. ∎

[a] This is the proof of Theorem 3.9 without the last line!

For completeness, we state without proof exactly which moduli have primitive roots.

**Theorem 3.19.** *$\mathbb{Z}_n^\times$ has a primitive root if and only if $n = 2, 4, p^k, 2p^k$ where $p$ is an odd prime.*

While lengthy, the proof is nicely constructive and shows the following:

- If $g$ is a primitive root modulo $p$, then at least one of $g$ or $g+p$ is a primitive root modulo $p^k$.
- If $g$ is a primitive root modulo $p^k$, then whichever of $g$ and $g+p^k$ is odd is a primitive root modulo $2p^k$.

Think about the examples on page 5 and see how they fit with this. One consequence of the Theorem, which isn't clear from our examples, is that comparatively few moduli have primitive roots!

**Example 3.20.** Find all the primitive roots modulo $50 = 2 \cdot 5^2$.

We know that 2 and 3 are primitive roots modulo 5. Therefore at least one each of the pairs

$$(2, 2+5) = (2, 7), \quad (3, 3+5) = (3, 8)$$

are primitive roots modulo 25. Quickly checking

$$\langle 3 \rangle = \{3, 9, 2, 6, 18, 4, 12, 11, 8, 24, \ldots\}$$

has $3^{10} \equiv -1 \pmod{25}$, whence 3 is a primitive root modulo 25. Since 3 is odd, it must also be a primitive root modulo 50. Indeed

$$\langle 3 \rangle = \{3, 9, 27, 31, 43, 29, 37, 11, 33, 49, 47, 41, 23, 19, 7, 21, 13, 39, 17, 1\}$$

All primitive roots modulo 50 therefore have the form $3^k$ where $k$ is comprime to $\varphi(50) = 20$: the complete set is therefore

$$\{3, 3^3, 3^7, 3^9, 3^{11}, 3^{13}, 3^{17}, 3^{19}\} = \{3, 27, 37, 33, 47, 23, 13, 17\}$$

**Exercises** 1. Find all the primitive roots for the given moduli: do this systematically as in Example 3.20 rather than by guessing.

(a) Modulo $49 = 7^2$. (b) Modulo $54 = 2 \cdot 3^3$.

2. (a) Explain where the proof of Theorem 3.18 fails when the modulus is composite.

   (b) What are the orders of the elements in $\mathbb{Z}_8^\times$? If Theorem 3.18 applied to all positive integers, what should the orders of the elements be?

3. We prove Theorem 3.16. Suppose $g$ is a primitive root modulo $n$ so that $\mathbb{Z}_n^\times = \langle g \rangle$. Since $g$ is a primitive root, observe that

$$(g^k)^\alpha \equiv 1 \iff \varphi(n) \mid \alpha k$$

Use this to prove that $(g^k)^\alpha \equiv 1 \iff \frac{\varphi(n)}{d} \,\Big|\, \alpha$, where $d = \gcd\big(k, \varphi(n)\big)$.

4. Suppose that $I$ is an index modulo an odd prime $p$.

   (a) If $a, b$ satisfy $ab \equiv 1 \pmod{p}$, how are the indices $I(a), I(b)$ related to each other?

   (b) If $a, b$ satisfy $a + b \equiv 0 \pmod{p}$, how are the indices $I(a), I(b)$ related to each other? (*Hint: $\exists$ a unique $k \in \mathbb{Z}_{p-1}$ such that $I(p-1) = k$: what is it?*)

5. Let $p$ be an odd prime and let $g$ be a primitive root modulo $p$.

   (a) Prove that $g^k$ is a quadratic residue modulo $p$ if and only if $k$ is even.

   (b) Use (a) to give a quick proof that the product of two non-residues is a residue, and more generally that $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$.

   (c) Use (a) to give a quick proof of Euler's Criterion $a^{(p-1)/2} \equiv \left(\frac{a}{p}\right) \pmod{p}$.

6. Suppose that $p$ is prime.

   (a) If $k$ divides $p-1$, show that the congruence $x^k \equiv 1 \pmod{p}$ has exactly $k$ distinct solutions modulo $p$.

   (b) Consider the congruence $x^k \equiv a \pmod{p}$. Find a simple way to use the values of $k, p$ and the index $I(a)$ to determine how many solutions this congruence has.

   (c) The number 3 is a primitive root modulo the prime 1987. How many solutions are there to the congruence $x^{111} \equiv 729 \pmod{1987}$? (*Hint:* $729 = 3^6$.)

7. (Only if you've done Rings and Fields)

   (a) Suppose $p$ is an odd prime. You are given that $p^k$ has a primitive root for any $k \in \mathbb{N}$. To what elementary group is the group of units $\mathbb{Z}_{p^k}^\times$ isomorphic?

   (b) Prove that

$$(\mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_j})^\times \cong \mathbb{Z}_{m_1}^\times \times \cdots \times \mathbb{Z}_{m_j}^\times$$

   for any $m_i \in \mathbb{N}_{\geq 2}$. Otherwise said, the group of units of a direct product ring is precisely the direct product of the groups of units of the individual rings.

   (c) Suppose $n = p_1^{\mu_1} \cdots p_j^{\mu_j}$ is the unique prime decomposition of some *odd* $n \in \mathbb{N}_{\geq 3}$ (the $p_i$ are distinct primes). Use (b) to prove that $\mathbb{Z}_n^\times$ is cyclic if and only if $j = 1$.