1. **Introduction:** Just for reference, Sections 9.2 and 9.3 concern themselves with the existence of primitive roots. They’re quite technical so we’re going to omit them and go to this section which addresses what we can do with them.

We know in regular (non-modulus) arithmetic that:

\[ r^x = a \iff \log_r a = x \]

If we tried to write this in modular arithmetic what would it be?

\[ r^x \equiv a \mod m \iff ??? \]

It turns out this isn’t quite as easy and we can only do this sort of thing in very specific circumstances.

2. **Indices:**

(a) **Introduction:** Given a modulus \( m \) and a primitive root \( r \) we know that \( \{r, r^2, ..., r^{\phi(m)}\} \) lists, up to congruence, all integers relatively prime to \( m \). For example \( r = 3 \) is a primitive root of \( m = 14 \) which we can verify by observing that:

\[
\begin{align*}
3^1 &\equiv 3 \mod 14 \\
3^2 &\equiv 9 \mod 14 \\
3^3 &\equiv 13 \mod 14 \\
3^4 &\equiv 11 \mod 14 \\
3^5 &\equiv 5 \mod 14 \\
3^6 &\equiv 1 \mod 14 
\end{align*}
\]

which shows that \( \text{ord}_{14} = 6 = \phi(14) \) and consequently up to congruence powers of 3 give us all integers coprime to 14.

We can then see that \( r^x \equiv a \mod m \) has a solution iff \( a \in \mathbb{Z} \) is coprime to \( m \). For example in the above we can solve \( 3^a \equiv 11 \mod 14 \) but we can’t solve \( 3^a \equiv 6 \mod 14 \).

This leads to the following general definition:

(b) **Definition:** If \( r \) is a primitive root of \( m \) and if \( \gcd(a, m) = 1 \) then the exponent \( x \) with \( 1 \leq x \leq \phi(m) \) satisfying \( r^x \equiv a \mod m \) is called the index of \( a \mod m \) (with base \( r \)). This is sometimes also called the discrete logarithm of \( a \mod m \) (with base \( r \)) and often the “with base \( r \)” is omitted when it’s clear what the base is. This is denoted \( \text{ind}_r a \) which is awkward because there’s no \( m \) mentioned in the notation, as it’s usually clear from context.

**Example:** The above example can then clarify:

\[
\begin{align*}
3^1 &\equiv 3 \mod 14 ... \; \text{and so} \; \text{ind}_3 3 = 1 \\
3^2 &\equiv 9 \mod 14 ... \; \text{and so} \; \text{ind}_3 9 = 2 \\
3^3 &\equiv 13 \mod 14 ... \; \text{and so} \; \text{ind}_3 13 = 3 \\
3^4 &\equiv 11 \mod 14 ... \; \text{and so} \; \text{ind}_3 11 = 4 \\
3^5 &\equiv 5 \mod 14 ... \; \text{and so} \; \text{ind}_3 5 = 5 \\
3^6 &\equiv 1 \mod 14 ... \; \text{and so} \; \text{ind}_3 1 = 6 
\end{align*}
\]

Immediately from the definition we have the following:

**Theorem:** If \( a, b \) are coprime to \( m \) and \( r \) is a primitive root then:

i. \( r^{\text{ind}_r a} = a \)

ii. \( a \equiv b \mod m \) iff \( \text{ind}_r a = \text{ind}_r b \). Note that since indices are always between 1 and \( \phi(m) \) we can write this as \( a \equiv b \mod m \) iff \( \text{ind}_r a = \text{ind}_r b \mod \phi(m) \) without changing it at all. This will be insanely useful.
Proof: Immediate.

(c) Index Rules: Indices behave like logarithms (think logarithm laws) but there’s a quirk that arises from the order of \( r \), that being \( \phi(m) \). To see why this is consider the logarithm rule:

\[
\log_r(ab) = \log_r a + \log_r b
\]

It would be tempting to write:

\[
\text{ind}_r(ab) = \text{ind}_r a + \text{ind}_r b \quad \Leftarrow \text{Tempting!}
\]

However this is not quite right. Consider that with \( m = 14 \) and \( r = 3 \) if we put \( a = 13 \) and \( b = 5 \) then \( ab = 9 \mod 14 \) and the Tempting statement would say:

\[
\text{ind}_39 = \text{ind}_313 + \text{ind}_35
\]

\[2 = 3 + 5\]

\[2 = 8\]

Which is clearly false. However note that \( 2 \equiv 8 \mod 6 = \phi(m) = \text{ord}_{14}3 \).

In general we get the following:

**Theorem:** Let \( m \) be a modulus, \( r \) be a primitive root, and \( a,b \) be coprime to \( m \). Then we have:

(i) \( \text{ind}_r1 \equiv 0 \mod \phi(m) \)
(ii) \( \text{ind}_r(ab) \equiv \text{ind}_r a + \text{ind}_r b \mod \phi(m) \)
(iii) \( \text{ind}_r (a^k) \equiv k \text{ind}_r a \mod \phi(m) \)

Note that there is no version equivalent to \( \log_r(a/b) = \ldots \).

**Proof:** For (i) By Euler’s Theorem we know that \( r^{\phi(m)} \equiv 1 \mod m \) and so \( \text{ind}_r1 = \phi(m) = 0 \mod \phi(m) \).

For (ii) note first that by the definition of index:

\[
r^{\text{ind}_r(ab)} \equiv ab \mod m
\]

And also:

\[
r^{\text{ind}_r a + \text{ind}_r b} = r^{\text{ind}_r a}r^{\text{ind}_r b} = ab \mod m
\]

So that:

\[
r^{\text{ind}_r(ab)} \equiv r^{\text{ind}_r a + \text{ind}_r b} \mod m
\]

Then by a theorem from Section 9.1 (which states that \( a^x \equiv a^y \mod m \) iff \( x \equiv y \mod \text{ord}_m a \)) we get:

\[
\text{ind}_r(ab) \equiv \text{ind}_r a + \text{ind}_r b \mod \phi(m)
\]

For (iii) note first that by the definition of index:

\[
r^{\text{ind}_r(a^k)} \equiv a^k \mod m
\]

And also:

\[
r^{k \text{ind}_r a} = (r^{\text{ind}_r a})^k \equiv a^k \mod m
\]

So that:

\[
r^{\text{ind}_r(a^k)} \equiv r^{k \text{ind}_r a} \mod m
\]

Then by the same theorem we get:

\[
\text{ind}_r(a^k) \equiv k \text{ind}_r a \mod \phi(m)
\]

QED
3. The Discrete Logarithm Problem and Tables: Given a modulus \( r \) and some \( a \) with \( \gcd(a, m) = 1 \) how difficult is it to find \( \text{ind}_ra \)? In other words how can we find \( x \) with \( r^x \equiv a \mod m \)? It turns out that it’s basically as difficult as trying all of \( 1, 2, 3, ..., \phi(m) \). There’s no real shortcut and in fact methods of encryption are based on the fact that it’s easy to do powers and hard to do indices.

So for the examples we do we’ll simply have to make up a table so that we have the indices are our disposal. For example the table for \( m = 14 \) and \( r = 3 \) would be:

<table>
<thead>
<tr>
<th>( a \mod 14 )</th>
<th>( 1 )</th>
<th>( 3 )</th>
<th>( 5 )</th>
<th>( 9 )</th>
<th>( 11 )</th>
<th>( 13 )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( \text{ind}_3a )</td>
<td>( 6 )</td>
<td>( 1 )</td>
<td>( 5 )</td>
<td>( 2 )</td>
<td>( 4 )</td>
<td>( 3 )</td>
</tr>
</tbody>
</table>

4. Index Arithmetic: We can use indices to solve modular problems involving exponents. These work pretty smoothly as long as we are careful about the moduli we’re dealing with. Remember the insanely important theorem from earlier:

\[
\text{ind}_ra \equiv \text{ind}_rb \mod \phi(m) \iff a \equiv b \mod m
\]

**Example:** Let’s solve \( 3x^{10} \equiv 12 \mod 17 \). First we obtain a primitive root for \( m = 17 \). Some work shows us that \( r = 3 \) works. Next we construct a table which has 16 entries because all \( 1 \leq a \leq 16 \) are coprime to 17. This also takes a lot of work, it’s not obvious:

| \( a \mod 17 \) | \( 1 \) | \( 2 \) | \( 3 \) | \( 4 \) | \( 5 \) | \( 6 \) | \( 7 \) | \( 8 \) | \( 9 \) | \( 10 \) | \( 11 \) | \( 12 \) | \( 13 \) | \( 14 \) | \( 15 \) | \( 16 \) |
|-----------------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|
| \( \text{ind}_3a \) | \( 16 \) | \( 14 \) | \( 1 \) | \( 12 \) | \( 5 \) | \( 15 \) | \( 11 \) | \( 10 \) | \( 2 \) | \( 3 \) | \( 7 \) | \( 13 \) | \( 4 \) | \( 9 \) | \( 6 \) | \( 8 \) |

We then proceed as follows:

\[
3x^{10} \equiv 12 \mod 17
\]

\[
\text{ind}_3(3x^{10}) \equiv \text{ind}_312 \mod 16
\]

\[
\text{ind}_33 + 10\text{ind}_3x \equiv \text{ind}_312 \mod 16
\]

\[
1 + 10\text{ind}_3x \equiv 13 \mod 16
\]

\[
10\text{ind}_3x \equiv 12 \mod 16
\]

This is a linear system if we treat \( \text{ind}_3x \) as the variable. Since \( \gcd(10, 16) = 2 | 12 \) there are 2 incongruent solutions mod 16. Work omitted these are:

\[
\text{ind}_3x \equiv 6, 14 \mod 16
\]

And so we can un-index:

\[
x \equiv 15, 2 \mod 17
\]

**Example:** Let’s solve \( 4^x \equiv 16 \mod 17 \). Don’t just eyeball and assume the only answer is \( x = 2 \)! We have a primitive root for \( m = 17 \) and a table already so we just go for it:

\[
4^x \equiv 16 \mod 17
\]

\[
\text{ind}_4(4^x) \equiv \text{ind}_416 \mod 16
\]

\[
x\text{ind}_44 \equiv \text{ind}_416 \mod 16
\]

\[
x(12) \equiv 8 \mod 16
\]

\[
12x \equiv 8 \mod 16
\]

\[
3x \equiv 2 \mod 4
\]

This is also a linear system but it’s more familiar since \( x \) is the variable. Since \( \gcd(3, 4) = 1 \mod 4 \) there is 1 incongruent solution mod 4 and that is \( x = 2 \).

So it did turn out that \( x = 2 \) is the solution but that is only true mod 4. There are lots of solutions, \( x = ..., -6, -2, 2, 6, 10, ... \)