Math 406 Section 9.4: Discrete Logarithms

1. **Introduction:**

   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?

   $$r^x \equiv a \bmod m \iff ???$$

   It turns out this isn't quite as easy and we can only do this in very specific circumstances.

2. **Indices:**

   (a) **Introduction:**

   Given a primitive root r of a modulus m we know that $\{r, r^2, ..., r^{\phi(m)}\}$ lists, up to congruence mod m, all integers coprime to m.

   Example:

   We see that $r = 3$ is a primitive root of the modulus $m = 14$ (with $\phi(14) = 6$):

   $$\{3^1, 3^2, 3^3, 3^4, 3^5, 3^6\} \equiv \{3, 9, 13, 11, 5, 1\} \bmod 14$$

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

   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 unique exponent x with $1 \leq x \leq \phi(m)$ satisfying $r^x \equiv a \bmod m$ 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:

   $$\begin{gathered}
   3^1 \equiv 3 \bmod 14 \text{ ... and so } \text{ind}_3 3 = 1 \\
   3^2 \equiv 9 \bmod 14 \text{ ... and so } \text{ind}_3 9 = 2 \\
   3^3 \equiv 13 \bmod 14 \text{ ... and so } \text{ind}_3 13 = 3 \\
   3^4 \equiv 11 \bmod 14 \text{ ... and so } \text{ind}_3 11 = 4 \\
   3^5 \equiv 5 \bmod 14 \text{ ... and so } \text{ind}_3 5 = 5 \\
   3^6 \equiv 1 \bmod 14 \text{ ... and so } \text{ind}_3 1 = 6
   \end{gathered}$$

   Note that, for example, $3^7 \equiv 3 \bmod 14$ as well but we wouldn't say that the index is 7 because the index has to be between 1 and $\phi(14) = 6$ inclusive.

   Immediately from the definition we have the following:

   (c) **Theorem:**

   If a, b are coprime to m and r is a primitive root mod m then:

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

   (ii) $a \equiv b \bmod m \iff \text{ind}_r a = \text{ind}_r b \iff \text{ind}_r a \equiv \text{ind}_r b \bmod \phi(m)$.

   Proof:

   Immediate. $\mathcal{QED}$

(d) **Index Rules:** Indices behave like logarithms except for a quirk. To see why this is consider the logarithm rule:

$$\log_r(ab) = \log_r a + \log_r b$$

It would be tempting to write:

$$\text{ind}_r(ab) = \text{ind}_r a + \text{ind}_r b \;\Leftarrow \text{Tempting!}$$

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

$$\begin{aligned} \text{ind}_3 9 &= \text{ind}_3 13 + \text{ind}_3 5 \\ 2 &= 3 + 5 \end{aligned}$$

Which is clearly false. However note that $2 \equiv 3 + 5 \bmod 6 = \phi(m)$.
In general we get the following:
Theorem:
Let r be a primitive root mod m and let a, b be coprime to m. Then we have:
(i) $\text{ind}_r 1 = \phi(m) \equiv 0 \bmod \phi(m)$
(ii) $\text{ind}_r(ab) \equiv \text{ind}_r a + \text{ind}_r b \bmod \phi(m)$
(iii) $\text{ind}_r \left(a^k\right) \equiv k \cdot \text{ind}_r a \bmod \phi(m)$
Note that there is no obvious version equivalent to $\log_r(a/b) = \ldots.$ Can you think of one?
Proof:
For (i) By Euler's Theorem we know $r^{\phi(m)} \equiv 1 \bmod m$ and so $\text{ind}_r 1 = \phi(m) \equiv 0 \bmod \phi(m)$.
For (ii) note first that by the definition of index:

$$r^{\text{ind}_r(ab)} \equiv ab \bmod m$$

And also:

$$r^{\text{ind}_r a + \text{ind}_r b} = r^{\text{ind}_r a} r^{\text{ind}_r b} \equiv ab \bmod m$$

So that:

$$r^{\text{ind}_r(ab)} \equiv r^{\text{ind}_r a + \text{ind}_r b} \bmod m$$

Then by a Theorem from Section 9.1 ($a^x \equiv a^y \bmod m$ iff $x \equiv y \bmod \text{ord}_m a$) we get:

$$\text{ind}_r(ab) \equiv \text{ind}_r a + \text{ind}_r b \bmod \phi(m)$$

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

$$r^{\text{ind}_r(a^k)} \equiv a^k \bmod m$$

And also:

$$r^{k \cdot \text{ind}_r a} = \left(r^{\text{ind}_r a}\right)^k \equiv a^k \bmod m$$

So that:

$$r^{\text{ind}_r(a^k)} \equiv r^{k \cdot \text{ind}_r a} \bmod m$$

Then by the same theorem we get:

$$\text{ind}_r(a^k) \equiv k \cdot \text{ind}_r a \bmod \phi(m)$$

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 $\text{ind}_r a$? In other words how can we find x with $r^x \equiv a \bmod m$? 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:

a	1	3	5	9	11	13
$\text{ind}_3 a$	6	1	5	2	4	3

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:

$$a \equiv b \bmod m \iff \text{ind}_r a = \text{ind}_r b \bmod \phi(m)$$

   Example: Let's solve $3x^{10} \equiv 12 \bmod 17$. 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 $1 \le a \le 16$ are coprime to 17. This also takes a lot of work, it's not obvious:

$a \bmod 17$	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$\text{ind}_3 a$	16	14	1	12	5	15	11	10	2	3	7	13	4	9	6	8

   We then proceed as follows:

$$\begin{aligned} 3x^{10} &\equiv 12 \bmod 17 \\ \text{ind}_3(3x^{10}) &\equiv \text{ind}_3 12 \bmod 16 \\ \text{ind}_3 3 + 10\text{ind}_3 x &\equiv \text{ind}_3 12 \bmod 16 \\ 1 + 10\text{ind}_3 x &\equiv 13 \bmod 16 \\ 10\text{ind}_3 x &\equiv 12 \bmod 16 \end{aligned}$$

   This is a linear system if we treat $\text{ind}_3 x$ as the variable. Since $\gcd(10, 16) = 2 \mid 12$ there are 2 incongruent solutions mod 16. Work omitted these are:

$$\text{ind}_3 x \equiv 6, 14 \bmod 16$$

   And so we can un-index:

$$x \equiv 15, 2 \bmod 17$$

   Example: Let's solve $4^x \equiv 16 \bmod 17$. 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:

$$\begin{aligned} 4^x &\equiv 16 \bmod 17 \\ \text{ind}_3(4^x) &\equiv \text{ind}_3 16 \bmod 16 \\ x\text{ind}_3 4 &\equiv \text{ind}_3 16 \bmod 16 \\ x(12) &\equiv 8 \bmod 16 \\ 12x &\equiv 8 \bmod 16 \\ 3x &\equiv 2 \bmod 4 \end{aligned}$$

   This is also a linear system but it's more familiar since x is the variable. Since $\gcd(3, 4) = 1 \bmod 4$ 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, $x = ..., -6, -2, 2, 6, 10, ...$