Discrete Logarithms

If $a$ is a primitive root mod $m$, then every element of $U_m$ is a power of $a$. We can exploit this fact to create the notion of a discrete logarithm:

The discrete logarithm or index of $x$ mod $m$ with base $a$, written $\text{ind}$, is the congruence class of $k$ mod $\varphi(m)$ where $x \equiv a^k \pmod{m}$.

The reason for the term logarithm should be clear:

**Proposition** If $a$ is a primitive root mod $m$, then
1. $\text{ind}_a 1 \equiv 0 \pmod{\varphi(m)}$;
2. $\text{ind}_a a \equiv 1 \pmod{\varphi(m)}$;
3. $\text{ind}_a (xy) \equiv \text{ind}_a x + \text{ind}_a y \pmod{\varphi(m)}$;
4. $\text{ind}_a x^n \equiv n \cdot \text{ind}_a x \pmod{\varphi(m)}$;
5. $\text{ind}_a x \equiv \text{ind}_a y \pmod{\varphi(m)} \iff x \equiv y \pmod{m}$.

**Proof of (5)** Seeing as how $x \equiv a^{\text{ind}_a x} \pmod{m}$ and $y \equiv a^{\text{ind}_a y} \pmod{m}$, we have $x \equiv y \pmod{m} \iff a^{\text{ind}_a x} \equiv a^{\text{ind}_a y} \pmod{m} \iff a^{\text{ind}_a x - \text{ind}_a y} \equiv 1 \pmod{m} \iff \varphi(m) \mid \text{ind}_a x - \text{ind}_a y \iff \text{ind}_a x \equiv \text{ind}_a y \pmod{\varphi(m)}$. //

We can then use the discrete logarithm to solve exponential equations in congruence arithmetic in the same way that we use continuous logarithms to solve real-valued exponential equations.
Example: \( 7^x \equiv 4 \pmod{17} \). We know that 3 is a primitive root \( \pmod{17} \), so we can use item (5) of the previous proposition to conclude that 

\[
x \cdot \text{ind}_3 7 \equiv \text{ind}_3 7^x \equiv \text{ind}_3 4 \pmod{16}.
\]

But from a table of indices base 3 we find that \( \text{ind}_3 7 \equiv 11 \pmod{16} \) and \( \text{ind}_3 4 \equiv 12 \pmod{16} \). So our condition reduces to \( 11x \equiv 12 \pmod{16} \), a linear congruence! This is easily solved to find \( x \equiv 4 \pmod{16} \).

Notice that we used a table of indices for a primitive root base in the example above. A straightforward computation of the powers of \( a \) \( \pmod{m} \) provides such a table, but it requires \( \varphi(m) \) power-reduction computations (raising \( a \) to the next highest power, then reducing \( \pmod{m} \)). Often in such problems, \( m = p \) is prime, whence we require \( p - 1 \) computational steps. Daniel Shanks has reduced the number of computations as follows:

There are \( p - 1 \) indices that must be computed; every index has a value in the range \( 0 \leq \text{ind}_a x \leq p - 2 \). If arranged row by row in a rectangular array, the array would be nearest to being a square array when it has \( n = \left\lfloor \sqrt{p-1} \right\rfloor \) columns in it (and \( \left\lfloor \sqrt{p-1} \right\rfloor \) rows), as we now show.
The entries in this array which lie in the first row of the table will be the first $n$ powers of the primitive root, $a^0, a^1, a^2, \ldots, a^{n-1} \mod(p-1)$, and the entries in the first column are the corresponding powers $a^0, a^n, a^{2n}, \ldots, a^{(q-1)n} \mod(p-1)$, where $q$ is the quotient in the division of $p-1$ by $n$ ($p-1 = qn + r, \ 0 \leq r < n$). Note that

\[
q = \left\lfloor \frac{p-1}{n} \right\rfloor = \left\lfloor \frac{p-1}{\sqrt{p-1}} \right\rfloor = \left\lfloor \sqrt{p-1} \right\rfloor
\]

so that the array will have $\left\lfloor \sqrt{p-1} \right\rfloor$ rows.

Now, to find the index for any $x$, it turns out that we do not need to compute the entire array of indices. Instead, we compute only the entries in the first column: $a^0, a^n, a^{2n}, \ldots, a^{qn} \mod(p-1)$, and then the $n$ values $a^{-r}x \equiv (a^{-1})^r x \mod p$ for $r = 0, 1, \ldots, n-1$. If some residue appears in both lists, then $a^{-j}x \equiv a^{in} \mod p$ for some choices of $i$ and $j$, $0 \leq i \leq q$, $0 \leq j < n$, whence $x \equiv a^{in+j} \mod p$ and $\text{ind}_ax \equiv in + j \mod (p-1))$. But of course, there must be a choice of $i$ and $j$ that satisfies this last congruence (by the division algorithm), so there will always be a unique such match.
Example: To solve the congruence $2^x \equiv 22 \pmod{37}$, first note that $2^{18} \equiv -1 \pmod{37}$, so that 2 is a primitive root mod 37. Then compute $\text{ind}_2 22$:

First, compute $n = \left\lfloor \sqrt{37} - 1 \right\rfloor = 6$.

Then, tabulate the powers $2^0, 2^1, 2^2, \ldots, 2^6 \pmod{37}$:

<table>
<thead>
<tr>
<th>$i$</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
</tr>
</thead>
<tbody>
<tr>
<td>$2^i \pmod{37}$</td>
<td>1</td>
<td>27</td>
<td>26</td>
<td>36</td>
<td>10</td>
<td>11</td>
</tr>
</tbody>
</table>

Next, tabulate the quantities $(2^{-1})^j 22 \pmod{37}$ for $0 \leq j \leq n - 1$, noting that $2^{-1} \equiv 19 \pmod{37}$:

<table>
<thead>
<tr>
<th>$j$</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
</tr>
</thead>
<tbody>
<tr>
<td>$19^j \cdot 22 \pmod{37}$</td>
<td>22</td>
<td>11</td>
<td>26</td>
<td>12</td>
<td>6</td>
<td>3</td>
</tr>
</tbody>
</table>

Since 11 is the unique common value in both lists, we get that $2^{5 \cdot 6} \equiv (2^{-1})^1 \cdot 22 \pmod{37}$, or $2^{5 \cdot 6 + 1} \equiv 22 \pmod{37}$, whence $x \equiv 31 \pmod{36}$.