1 Indices, Index Arithmetic, Discrete Logarithms

How can we solve (or even know if solutions exist) something like

$$3^x \equiv 5 \bmod 22$$

or -how many solutions there might be, or -if the solutions are mod 22 or something else. In pre-calculus with $3^x \equiv 5$ we can do $x = \log_3 5$, but we cannot do that here (yet).

1.1 The Order of an Integer & Primitive Roots

1. **Introduction:** The process of exponentiation and its inverse (logarithms) is as essential in modular arithmetic as it is in regular math and forms the basis for various encryption techniques. We begin by taking a base a which is coprime to a modulus m and looking at the powers of a mod m.

2. **Order:** Given a modulus m and an integer a with $\gcd(a, m) = 1$ Euler's Theorem tells us that $a^{\phi(m)} \equiv 1 \bmod m$. It does not however tell us that $\phi(m)$ is the lowest power which yields 1. This leads to the following.

   (a) **Definition:** Suppose $\gcd(a, m) = 1$ we define the *order* of a mod m as the smallest power x such that $a^x \equiv 1 \bmod m$. This is denoted $\text{ord}_m a$.
   Note: $\text{ord}_m a \leq \phi(m)$
   Note: We can say "order of a" when m is contextually obvious.
   Ex. Let's find $\text{ord}_{11} 3$. Well,

   $$\begin{aligned} 3^1 &\equiv 3 \bmod 11 \\ 3^2 &\equiv 9 \bmod 11 \\ 3^3 &\equiv 5 \bmod 11 \\ 3^4 &\equiv 4 \bmod 11 \\ 3^5 &\equiv 1 \bmod 11 \end{aligned}$$

   Thus, $\text{ord}_{11} 3 = 5$.
   Note: We can now start to see that the order gives us a pattern under which 3^x will repat!

   (b) **Theorem:** For $x \in \mathbb{Z}^+$ we have $a^x \equiv 1 \bmod m$ if and only if $x \equiv 0 \bmod \text{ord}_m a$ if and only if $\text{ord}_m a \mid x$.
   Ex. We saw $\text{ord}_{11} 3 = 5$ so $3^x \equiv 1 \bmod 11$ if and only if $x \equiv 0 \bmod 5$ if and only if $5 \mid x$.

Proof.
$\rightarrow$ Assume $a^x \equiv 1 \bmod m$, use the Divison Algorithm to write $x = q(\text{ord}_m a) + r$. Observe,

$$1 \equiv a^x \equiv \left(a^{\text{ord}_m a}\right)^q a^r \equiv a^r \bmod m$$

Since $\text{ord}_m a$ is the smallest positve power, we must have $r = 0$. Thus, $x = q\text{ord}_m a$ so $\text{ord}_m a \mid x$.

$\leftarrow$ Assume $\text{ord}_m a \mid x$. Then,

$$a^x \equiv a^{k\text{ord}_m a} \equiv \left(a^{\text{ord}_m a}\right)^k \equiv 1^k \equiv 1 \bmod m$$

□

(c) **Corollary:** We have $\text{ord}_m a \mid \phi(m)$.

Proof. The proof here is obvious because $a^{\phi(m)} \equiv 1 \bmod m$. Apply the theorem. □

So to find $\text{ord}_m a$ try divisors of $\phi(m)$ only.
Ex. To find $\text{ord}_{11} 2$ we note that $\phi(11) = 10$. So we need to check $1, 2, 5$ because if it fails for those, $\text{ord}_{11} 2 = 10$.

$$2^1 \equiv 2 \not\equiv 1 \bmod 11$$
$$2^2 \equiv 4 \not\equiv 1 \bmod 11$$
$$2^5 \equiv 10 \not\equiv 1 \bmod 11$$

Aha, from this we can see that $2^{10} \equiv 1 \bmod 11$ by Euler's Theorem. So $\text{ord}_{11} 2 = 10$.

(d) **Theorem:** We have $a^x \equiv a^y \bmod m$ if and only if $\text{ord}_m a \mid (x - y)$ if and only if $x \equiv y \bmod \text{ord}_m a$. i.e. Exponents work mod $\text{ord}_m a$.
Ex. $\text{ord}_{11} 3 = 5$ so $3^x \equiv 3^y \bmod 11$ if and only if $x \equiv y \bmod \text{ord}_{11} 3$ $(x \equiv y \bmod 5)$.

3. **Primitive Roots**