The Order of $a \mod m$

Recall the definition: the order of $a \mod m$ is the smallest positive integer $n = \text{ord}_m a$ that satisfies $a^n \equiv 1 \pmod{m}$ (in particular, note that $a$ has no order mod $m$ unless $(a,m) = 1$). As an immediate corollary of Euler’s Theorem, we have

**Proposition** If $a^k \equiv 1 \pmod{m}$, then $\text{ord}_m a \mid k$.

**Proof** Divide $k$ by $\text{ord}_m a$: we write $k = q \cdot \text{ord}_m a + r$, $0 \leq r < \text{ord}_m a$. Then

$$1 \equiv a^{q \cdot \text{ord}_m a + r} = (a^{\text{ord}_m a})^q a^r \equiv a^r \pmod{m}$$

so by the definition of order, we must have $r = 0$. //

This result has a number of useful consequences:

**Corollary** If $(a,m) = 1$, then $\text{ord}_m a \mid \varphi(m)$. In particular, if $p$ is prime and $(a,p) = 1$, then $\text{ord}_p a \mid p - 1$. //

**Example**: Evaluate $\text{ord}_{17} 3$. As $\text{ord}_{17} 3 \mid \varphi(17) = 16$, the only possibilities for $\text{ord}_{17} 3$ are 2, 4, 8, and 16. But $3^8 \equiv 9^4 \equiv 81^4 \equiv 13^2 \equiv -1 \pmod{17}$, so we must have $\text{ord}_{17} 3 = 16$. 
**Corollary** If \((a, m) = 1\) and \(a^i \equiv a^j \pmod{m}\), then \(i \equiv j \pmod{\text{ord}_m a}\).

**Proof** We may suppose \(i > j\). Then multiplication by \((a^{-1})^j\) yields \(a^{i-j} \equiv 1 \pmod{m}\). So \(\text{ord}_m a | (i - j)\). //

**Corollary** If \(n = \text{ord}_m a\), then \(1, a, a^2, \ldots, a^{n-1}\) are distinct \(\pmod{m}\). //

In fact, we now can formulate a relationship between the order of any number with respect to any modulus and the order of any power of that number.

**The Order Formula** If \((a, m) = 1\), then

\[
\text{ord}_m (a^k) = \frac{\text{ord}_m a}{(k, \text{ord}_m a)}.
\]

**Proof** Put \(l = \frac{\text{ord}_m a}{(k, \text{ord}_m a)}\). Then

\[
(a^k)^l = a^{kl} = (a^{\text{ord}_m a})^{k/(k, \text{ord}_m a)} \equiv 1 \pmod{m}
\]

from which we conclude that \(\text{ord}_m (a^k) \mid l\). But since 
\((a^k)^{\text{ord}_m (a^k)} \equiv 1 \pmod{m}\), we also can say that 
\(\text{ord}_m a \mid k \cdot \text{ord}_m (a^k)\). Dividing through by \((k, \text{ord}_m a)\),
we can write

\[ l = \frac{\text{ord}_m a}{(k, \text{ord}_m a)} \bigg| \frac{k}{(k, \text{ord}_m a)} \cdot \text{ord}_m (a^k) \]

and since \( l \) is relatively prime to \( \frac{k}{(k, \text{ord}_m a)} \), it follows that \( l \mid \text{ord}_m (a^k) \). Combined with our earlier conclusion that \( \text{ord}_m (a^k) \mid l \), we deduce that \( \text{ord}_m (a^k) = l \). This ends the proof. //

With this result, we can finally give a complete picture of the multiplicative structure of arithmetic mod \( m \) for many different values of \( m \). The congruence classes relatively prime to \( m \) (what we have identified as the set \( U_m \) of units mod \( m \)) are precisely the ones with multiplicative inverses (i.e., \( U_m \) is a group under multiplication mod \( m \)).

The situation is simplest as we have seen in the case of prime modulus.

*Example:* Consider \( U_{149} \), the (group of) units under multiplication modulo the prime 149. The smallest element in \( U_{149} \) is 1, but 1 trivially has order 1. The next smallest element is 2. But \( \text{ord}_{149} 2 \mid \phi(149) = 148 = 2^2 \cdot 37 \), so there are only a few possibilities
for this value. Since $2^{148/37} \equiv 2^4 = 16 \pmod{149}$ and $2^{148/2} \equiv 2^{74} = -1 \pmod{149}$, the order of 2 cannot be a proper factor of 148, so $\text{ord}_{149} 2 = 148$. It follows that 1, 2, $2^2$, ..., $2^{147}$ are distinct mod 149. But then these 148 numbers represent in a simple manner all of the congruence classes in $U_{149}$. (In the language of algebra, $U_{149}$ is a cyclic group generated by the element 2.)

Another way of seeing this: by Fermat’s Little Theorem, all 148 elements of $U_{149}$ are roots of the polynomial congruence $x^{148} \equiv 1 \pmod{149}$. But since every such element is, by the above computations, congruent to a power of 2 mod 149, the roots of this polynomial have the form $x = 2^k \pmod{149}$, for each $k$ from 0 to 147.

What is significant here is that 2 has maximal order in $U_{149}$; it is because of this that all the elements of $U_{149}$ can be represented as powers of 2, or that all roots of $x^{148} \equiv 1 \pmod{149}$ are powers of this one root. For this reason, we call 2 a primitive root mod 149.

If $(a, m) = 1$ and $\text{ord}_m a = \varphi(m)$, then $a$ is called a primitive root mod $m$. 
Note that

$$\text{ord}_{149}(2^k) = \frac{\text{ord}_{149} 2}{(k, \text{ord}_{149} 2)} = \frac{148}{(k, 148)}$$

so the orders of the elements of $U_{149}$ can be effectively computed.

For instance, when $k = 16$, we have $\text{ord}_{149}(2^{16}) = 37$, and when $k = 15$, we have $\text{ord}_{149}(2^{15}) = 148$. This means that $2^k$ is a primitive root mod 149 for any $k$ that is relatively prime to 148. We know that there are $\varphi(148) = \varphi(4)\varphi(37) = 2 \cdot 36 = 72$ such values!

Can we also describe the structure of the units modulo a composite number?

**Example:** Consider $U_{50}$. The smallest nontrivial element is 3, and $\text{ord}_{50} 3 | \varphi(50) = \varphi(2)\varphi(25) = 20$. But $3^{10} = 59049 \equiv -1 \pmod{50}$, so $\text{ord}_{50} 3$ is not a factor of 10, forcing $\text{ord}_{50} 3 = 20$. That is, 3 is a primitive root mod 50. Consequently, the 20 elements of $U_{50}$ can be represented as the congruence classes of the powers of 3 mod 50: 1, 3, 3^2, ..., 3^{19}.

However, it doesn’t always turn out so nice as this...