A Closer Look at Integers Modulo a Prime

Let $p$ be a prime number. There are $p$ elements of the integers modulo $p$:

$$\mathbb{Z}_p = \{[0]_p, [1]_p, \ldots, [p-1]_p\}.$$ 

We’ll act like mathematicians and drop the brackets.

We’ve seen how $\mathbb{Z}_p$ satisfies the “usual” axioms for addition and multiplication. But $\mathbb{Z}_p$ is really more like the rational numbers $\mathbb{Q}$ than integers $\mathbb{Z}$. Every non-zero element of $\mathbb{Z}_p$ is invertible.

From the theory of congruences (in particular, Proposition 1.3.4), we can always solve the congruence $ax \equiv 1 \pmod{p}$ if $p \nmid a$. In other words, if $a$ is a non-zero element of $\mathbb{Z}_p$, then $a$ has an inverse. (With brackets: $[a]_p$ is invertible if $[a]_p \neq [0]_p$.)

**Examples:** In $\mathbb{Z}_{13}$, the inverse of 2 is 7: $2 \cdot 7 = 1$. Here we’ve dropped the brackets because we’re lazy. More precisely, we’d write $[2]_{13} \cdot [7]_{13} = [1]_{13}$.

In $\mathbb{Z}_{23}$, the inverse of 5 is ...???
Take a non-zero element of $\mathbb{Z}_p$. Let’s call it $a$. Consider the powers of $a$: $a^1, a^2, a^3, \ldots$, which are all elements of $\mathbb{Z}_p$. Moreover, none of them are zero (in $\mathbb{Z}_p$). Why?

There are only $p-1$ non-zero elements of $\mathbb{Z}_p$, but we have infinitely many powers of $a$. Clearly, these powers must repeat.

For example, the powers of 3 in $\mathbb{Z}_{19}$ are:

\[
3^1, \quad 3^2 = 9, \quad 3^3 = 27 = 8, \quad 3^4 = 24 = 5, \quad 3^5 = 15,
\]
\[
3^6 = 45 = 7, \quad 3^7 = 21 = 2, \quad 3^8 = 6, \quad 3^9 = 18 = -1.
\]

We now see that $3^{18} = (3^9)^2 = -1^2 = 1$, so $3^{19} = 3$.

The remaining powers are

\[
3^{10} = -3 = 16, \quad 3^{11} = -9 = 10, \quad 3^{12} = -8 = 11, \quad 3^{13} = -5 = 14,
\]
\[
3^{14} = -15 = 4, \quad 3^{15} = -7 = 12, \quad 3^{16} = -2 = 17, \quad 3^{17} = -6 = 13
\]

Notice how every non-zero element of $\mathbb{Z}_{19}$ is actually a power of 3. That makes multiplication much simpler! Instead of using $0, \ldots, 18$ as elements (more precisely, representatives of the congruence classes), we could use 0 and the 18 powers of 3: $3^1, 3^2, \ldots, 3^{18}$.

One example of the power of this idea is to consider $a^{19}$ in $\mathbb{Z}_{19}$.

So all the non-zero elements of $\mathbb{Z}_{19}$ are just powers of 3. Are there other numbers besides 3 which would work the same way? Is there some sort of congruence going on with the exponents?