Theorem 1. For any prime number $p$, there are exactly two non-isomorphic rings of order $p$.

Proof. All rings are additive Abelian groups. The only group of order $p$ is the cyclic group $\mathbb{Z}_p$. This group is generated by 1. Let $R$ be a ring of order $p$. Then, without loss of generality, $R$ is identical to $\mathbb{Z}_p$ as far as the additive structure is concerned, though $R$ may have a different multiplicative structure. Because of the distributivity axiom and because 1 generates $R$, multiplication in $R$ is completely determined by the product of 1 with itself, for example, $2 \times 3 = (1 + 1) \times (1 + 1 + 1) = 6 \cdot (1 \times 1)$, where $\times$ is the multiplication operation on the ring and $n \cdot x$ is shorthand for the repeated addition $x + x + \cdots + x(n \text{ times})$. This shorthand provided by the $\cdot$ operator could also be interpreted as the scalar multiplication in a $\mathbb{Z}$-module. Since there can be at most $p$ values assigned to $1 \times 1$, there can be at most $p$ non-isomorphic rings of order $p$.

Suppose $R$ had the multiplication $\times_a$ defined as follows. Define $x \times_a y = a \cdot xy$, where the implied multiplication refers to standard multiplication in $\mathbb{Z}_p$. This operation is obviously well-defined. We must show that $\times_a$ is associative, and distributive.

\[
x \times_a (y + z) = a \cdot x(y + z) \\
= a \cdot (xy + xz) \\
= a \cdot xy + a \cdot xz \\
= x \times_a y + x \times_a z
\]

This proves that $\times_a$ is left-distributive. It is also right-distributive. Associativity is also simple to prove.

\[
(x \times_a y) \times_a z = (a \cdot xy) \times_a z \\
= a \cdot (a \cdot xyz) \\
= a^2 \cdot (xyz)
\]

Similarly,

\[
x \times_a (y \times_a z) = x \times_a (a \cdot yz) \\
= a \cdot (a \cdot xyz) \\
= a^2 \cdot (xyz)
\]

Thus associativity is proven. Notice that as $a$ ranges from 0 to $p - 1$, $1 \times_a 1$ ranges from 0 to $p - 1$. When $a = 0$, the ring becomes the trivial ring.
where the multiplication is defined to be identically 0. If \( a \neq 0 \), then \( R \) is ring-isomorphic to \( \mathbb{Z}_p \), regardless of the value of \( a \). This we now prove.

Define the function \( \phi_{a^{-1}} : (\mathbb{Z}_p, +, \times) \rightarrow (R, +, \times_{a}) \) by setting \( \phi_{a^{-1}}(x) = a^{-1} \cdot x \). Here \( a^{-1} \) refers to the multiplicative inverse of \( a \) in the field \( \mathbb{Z}_p \). Note that \( \phi_{a}(\phi_{a^{-1}}(x)) = \phi_{a^{-1}}(\phi_{a}(x)) = x \), so \( \phi_{a^{-1}} \) has a 2-sided inverse and is, therefore, bijective. We now prove that \( \phi_{a^{-1}} \) homomorphism.

\[
\phi_{a^{-1}}(x) \times_{a} \phi_{a^{-1}}(y) = (a^{-1} \cdot x) \times_{a} (a^{-1} \cdot y) \\
= a \cdot (a^{-2} \cdot xy) \\
= a^{-1} \cdot xy \\
= \phi_{a^{-1}}(xy)
\]

This establishes that \( \phi_{a^{-1}} \) is an isomorphism. Thus the theorem is proven. The only two truly different rings of order \( p \) are \( \mathbb{Z}_p \) with standard multiplication and trivial multiplication. \( \square \)