Generally speaking, if you are given two rings $R$ and $S$ and asked are they isomorphic, the answer should be: No. It’s easier to show they are not isomorphic than to show they are! For example, there are $25!$ one to one correspondences between two fields $\mathbb{Z}_5[x]_{x^2+2}$ and $\mathbb{Z}_5[y]_{y^2+3}$. That number is huge. For example, $25!$ seconds is more than $10^{15}$ years! Not every one to one correspondence however is an isomorphism and there are just two isomorphisms between these two rings. How to find those two maps from those $25!$?

To show two rings are not isomorphic, on the other hand, all one needs to do is to find an algebraic property that one ring has that the other ring does not have. So for example $\mathbb{Z}$ is not isomorphic to $\mathbb{Z} \oplus \mathbb{Z}$ because $\mathbb{Z}$ is an integral domain, while $\mathbb{Z} \oplus \mathbb{Z}$ has zero divisors. For $(2,0)(0,3) = (0,0) \in \mathbb{Z} \oplus \mathbb{Z}$. In general, the ring $R \oplus S$ is more complicated than $R$ and $S$, in a number of ways. For example $R \oplus S$ has zero divisors for all rings $R, S$ even if $R$ and $S$ are integral domains. For $(1_R,0_S)(0_R,1_S) = (0_R,0_S)$.

An isomorphism is not just any old one to one correspondence. It must carry 0 to 0 and 1 to 1. So though there are $10!$ one to one correspondences from a ring with 10 elements to another ring with 10 elements, there are at most $8!$ isomorphisms, because $0 \to 0$ and $1 \to 1$, Still are large number to check, but smaller than before!

**Lemma 43**

(i) There is only one element 0 in any ring $R$ which satisfies A2 (in the Ring axioms).

(ii) For every $x$, there is only one element $-x$ in any ring $R$ which satisfies A3 (in the Ring axioms).

(iii) There is only one element 1 in any ring $R$ which satisfies M2 (in the Ring axioms).

(iv) If $x \in \mathbb{R}$ has an inverse $x^{-1} \in \mathbb{R}$, then $x^{-1}$ is unique.

**Proof.**

(i) Suppose that 0 and 0’ satisfy the axioms A, including A2. Then

$$0' = 0' + 0 = 0.$$

(ii) Suppose that there exists $x \in \mathbb{R}$ with two possible additive inverses $-x$ and $x'$. Then

$$x' = x' + 0 = x' + (x + (-x)) = (x' + x) + (-x) = 0 + (-x) = -x.$$

(iii) Suppose that 1 and 1’ satisfy M2. Then

$$1' = 11' = 1'.$$
(iv) If \( x \in \mathbb{R} \) has an inverse \( x^{-1} \in \mathbb{R} \), and suppose that \( xy = yx = 1 \in \mathbb{R} \). Consider
\[
y = 1.y = (x^{-1}x)y = x^{-1}(xy) = x^{-1}.1 = x^{-1}.
\]
This completes the proof.

**Lemma 44** Given an isomorphism \( \varphi : R \to S \) then \( \varphi(0_R) = 0_s \) and \( \varphi(1_R) = 1_s \).

**Proof.** First \( \varphi(0_R) + 0_s = \varphi(0_R) = \varphi(0_R + 0_R) = \varphi(0_R) + \varphi(0_R) \) and adding \( -\varphi(0_R) \) to both sides of this equation, we get \( \varphi(0_R) = 0_s \).

Next as an isomorphism \( \varphi \) is an onto map, that is, every element \( x \) in the target ring \( S \) has the form \( \varphi(r) \) for some \( r \in R \).

So if \( x \in S \), \( x = \varphi(r) \), for some \( r \in R \), and
\[
x = \varphi(r) \\
= \varphi(1_R r) \\
= \varphi(1_R) \varphi(r) \\
= \varphi(1_R) x \\
= x. \varphi(1_R), \text{ for all } x \in \mathbb{R}.
\]
Thus \( \varphi(1_R) \) satisfies the axiom M2 for rings.

But there is only one element which satisfies M2 in any ring by Lemma 44(iii). Hence \( \varphi(1_R) = 1_s \).

This completes the proof.

**Lemma 45** If \( \varphi : R \to S \) is an isomorphism, then \( \varphi(-x) = -\varphi(x) \) and \( \varphi(y^{-1}) = (\varphi(y))^{-1} \) if \( y \) is a unit in \( R \).

**Proof.** \( 0_s = \varphi(0_R) = \varphi(x + (-x)) = \varphi(x) + \varphi(-x) \) and adding \( -\varphi(x) \) to both sides we have \( -\varphi(x) = \varphi(-x) \), for \( x \in R \).

Suppose that \( y \) is a unit in \( R \) and \( yz = 1_R \). Then \( 1_s = \varphi(1_R) = \varphi(yz) = \varphi(y) \varphi(z) \) and so \( \varphi(y)^{-1} = \varphi(z) \), since by Lemma 43(iv), inverses are unique, if they exist.

This completes the proof.

So isomorphisms take additive inverses (and multiplicative inverses, if they exist) to additive (and multiplicative) inverses.

I want us to look at the rings \( \mathbb{Z}_3 \) and \( \mathbb{Z}_4 \) and \( \mathbb{Z}_3 \oplus \mathbb{Z}_4 \) more carefully. This last ring has 12 elements:
\[
(0,0), (0,1), (0,2), (0,3), (1,0), (1,1), (1,2), (1,3), (2,0), (2,1), (2,2), (2,3).
\]
We know another ring with 12 elements, namely \( \mathbb{Z}_{12} \). The question: Is \( \mathbb{Z}_3 \oplus \mathbb{Z}_4 \) isomorphic to \( \mathbb{Z}_{12} \) should have the answer No, by the 51% principle. But that would be wrong. In fact they are isomorphic!

You see that by Lemma 44, an isomorphism must carry 0 to 0 and 1 to 1, and so if we could find an isomorphism \( \varphi : \mathbb{Z}_{12} \to \mathbb{Z}_3 \oplus \mathbb{Z}_4 \), then we must have \( \varphi(0) = (0,0) \) and \( \varphi(1) = (1,1) \).
Further then it follows that we must have $\varphi(2) = \varphi(1 + 1) = \varphi(1) + \varphi(1) = (2, 2)$. And so on. We get

\begin{align*}
0 &\rightarrow (0, 0) \\
1 &\rightarrow (1, 1) \\
2 &\rightarrow (2, 2) \\
3 &\rightarrow (0, 3) \\
4 &\rightarrow (1, 0) \\
5 &\rightarrow (2, 1) \\
6 &\rightarrow (0, 2) \\
7 &\rightarrow (1, 3) \\
8 &\rightarrow (2, 0) \\
9 &\rightarrow (0, 1) \\
10 &\rightarrow (1, 2) \\
11 &\rightarrow (2, 3).
\end{align*}

Indeed this is an isomorphism. It remembers both addition and multiplication and $\mathbb{Z}_{12} \cong \mathbb{Z}_3 \oplus \mathbb{Z}_4$.

**Theorem 46 (Chinese Remainder Theorem)** If $n = ab$, where $(a, b) = 1$, then $\mathbb{Z}_n \cong \mathbb{Z}_a \oplus \mathbb{Z}_b$.

Remark. This is true for our other favourite rings, eg $\mathbb{Z}[i]$ and $\mathbb{Z}_p[x]$, with essentially the same proof. I won’t give that detail here, however for example: $\mathbb{Z}[i]_{(2+3i)(4+i)} \cong \mathbb{Z}[i]_{2+3i} \oplus \mathbb{Z}[i]_{4+i}$ and $\mathbb{Z}_p[x]_{f(x)g(x)} \cong \mathbb{Z}_p[x]_{f(x)} \oplus \mathbb{Z}_p[x]_{g(x)}$, if $(f(x), g(x)) = 1$, for example.

**Proof.** Define $\varphi : \mathbb{Z}_n \rightarrow \mathbb{Z}_a \oplus \mathbb{Z}_b$. by $\varphi(k) = (k, k)$, for $k \in \mathbb{Z}_n$.

Then $\varphi$ is an isomorphism.

1. $\varphi$ is one to one. For suppose that $\varphi(x) = \varphi(y)$. Then $(x, x) = (y, y)$ and so $(x - y, x - y) = (0, 0)$. Hence $x - y \equiv 0 \pmod{a}$ and $x - y \equiv 0 \pmod{b}$. Thus $x - y = ka$ is a multiple of $b$, $b|ka$ and since $(a, b) = 1$, it follows by Lemma 24 that $b|k$ and so $k = \ell b$ and $x - y = ka = \ell ab$ and $x - y \equiv 0 \pmod{ab}$. Thus $x = y \in \mathbb{Z}_n$.

2. $\varphi$ is onto. Since $\mathbb{Z}_n$ has $n$ elements as does $\mathbb{Z}_a \oplus \mathbb{Z}_b$, and $\varphi$ is a one to one map of $\mathbb{Z}_n$ into it, it takes $n$ different things from $\mathbb{Z}_n$ to $n$ different things in $\mathbb{Z}_a \oplus \mathbb{Z}_b$. Hence every element of $\mathbb{Z}_a \oplus \mathbb{Z}_b$ is $\varphi(x)$ for some $x \in \mathbb{Z}_n$. It follows that $\varphi$ maps $\mathbb{Z}_n$ onto $\mathbb{Z}_a \oplus \mathbb{Z}_b$.

Hence $\varphi$ is a one to one correspondence.

3. $\varphi$ remembers addition. For $\varphi(x + y) = (x + y, x + y) = (x, x) + (y, y) = \varphi(x) + \varphi(y)$.

4. $\varphi$ remembers multiplication. For $\varphi(xy) = (xy, xy) = (x, x)(y, y) = \varphi(x)\varphi(y)$.

Therefore $\varphi$ is an isomorphism and $\mathbb{Z}_n \cong \mathbb{Z}_a \oplus \mathbb{Z}_b$.

This completes the proof.

Remark. It is interesting here to stop and ask: Whatever does this have to do with the Chinese Remainder Theorem? On the face of it, it appears to be on quite another planet! Well, that’s not true. It turns out that the Chinese Remainder Theorem we know and love is actually point 2 in the proof above!
For since $\varphi$ maps $\mathbb{Z}_n$ onto $\mathbb{Z}_a \oplus \mathbb{Z}_b$ it follows that every element $(x, y)$ has the form $\varphi(X) = (X, X)$ for some $X \in \mathbb{Z}_n$. But that just asserts that $X \equiv x \pmod{a}$, and $X \equiv y \pmod{b}$, the CRT!.

But Theorem 46 is a much stronger statement than the first formulation of CRT. It asserts that the algebra $\mathbb{Z}_n$ is exactly built out of $\mathbb{Z}_a$ and $\mathbb{Z}_b$, that every algebraic question one can ask about $\mathbb{Z}_n$ can be answered by looking in $\mathbb{Z}_a$ and $\mathbb{Z}_b$ and then going back to $\mathbb{Z}_n$. 