The Chinese Remainder Theorem

Let's start by restating Theorem 15.1.15 in the case $p = 2$:

Chinese Remainder Theorem: Let n_1 and n_2 be integers that have no common factor greater than 1. Let $n = n_1 n_2$. Define

$$\theta : \mathbb{Z}_n \to \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2}$$

by

$$\theta(k) = (k_1, k_2)$$

where $0 \leq k_1 < n_1$, $0 \leq k_2 < n_2$, $k \equiv k_1 \pmod{n_1}$, and $k \equiv k_2 \pmod{n_2}$. (That is, k_1 is the remainder you get when you divide k by n_1, and k_2 is the remainder you get when you divide k by n_2.) Then θ is an isomorphism from $\mathbb{Z}_n$ into $\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2}$.

Recall that an isomorphism between two groups $[G_1; *_1]$ and $[G_2; *_2]$ is a bijection f from G_1 to G_2 with the property that $f(a *_1 b) = f(a) *_2 f(b)$ for all a, b in G_1.

Let's understand the Chinese Remainder Theorem in the case $n_1 = 2$ and $n_2 = 3$. $*_1$ is $+_6$ (mod 6 addition), and $*_2$ (let's just write it as $*$) is the direct product operation $(x, y) * (x', y') = (x +_2 x', y +_3 y')$. Let θ be the function from $\mathbb{Z}_6$ to the direct product $\mathbb{Z}_2 \times \mathbb{Z}_3$ given by the table below, showing k versus $\theta(k) = (k_1, k_2)$, where $0 \leq k_1 < 2$, $0 \leq k_2 < 3$, $k_1 \equiv k \pmod{2}$, and $k_2 \equiv k \pmod{3}$:

k	$\theta(k) = (k_1, k_2)$
0	$(0, 0)$
1	$(1, 1)$
2	$(0, 2)$
3	$(1, 0)$
4	$(0, 1)$
5	$(1, 2)$

cc

Theorem 15.1.15 says that θ is an isomorphism of $\mathbb{Z}_6$ with the direct product $\mathbb{Z}_2 \times \mathbb{Z}_3$. That is, $\theta(a +_6 b) = \theta(a) * \theta(b)$ for all a, b in $\mathbb{Z}_6$.

Let's check this in 1 (out of 6×6) cases. Does $\theta(3 +_6 4)$ equal $\theta(3) * \theta(4)$? I.e., does $\theta(1)$ equal $(1, 0) * (0, 1)$? I.e., does $(1, 1)$ equal $(1 + 20, 0 + 31)$? Yes!

(Look back at the notes for lecture #12: There we constructed an isomorphism between $\mathbb{Z}_6$ and $\mathbb{Z}_2 \times \mathbb{Z}_3$ by treating the two groups as cyclic groups, generated by 1 and (1,1), respectively.)