

The Chinese Remainder Theorem

Let's understand Theorem 15.1.15 in the case $p = 2$. The Theorem says: Let n_1 and n_2 be integers that have no common factor greater than 1. Let $n = n_1 n_2$. Define

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

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 where $n_1 = 2$ and $n_2 = 3$. $*_1$ is $+_6$ (mod 6 addition), the standard operation on \mathbb{Z}_6 , and $*_2$ is $+_{2,3}$, the direct product operation on $\mathbb{Z}_2 \times \mathbb{Z}_3$ given by the formula $(x, y) +_{2,3} (x', y') = (x +_2 x', y +_3 y')$. 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)

Theorem 15.1.15 says that θ is an isomorphism from \mathbb{Z}_6 to the direct product $\mathbb{Z}_2 \times \mathbb{Z}_3$. That is, θ is a bijection (that's easy to see) and $\theta(a +_6 b) = \theta(a) +_{2,3} \theta(b)$ for all a, b in \mathbb{Z}_6 . Let's use the table to check that the equation holds in one case (out of $6 \times 6 = 36$ cases). Does $\theta(3 +_6 5)$ equal $\theta(3) +_{2,3} \theta(5)$? I.e., does $\theta(2)$ equal $(1, 0) +_{2,3} (1, 2)$? I.e., does $(0, 2)$ equal $(1 +_2 1, 0 +_3 2)$? It does.

Also, the inverse function θ^{-1} is an isomorphism from $\mathbb{Z}_2 \times \mathbb{Z}_3$ to \mathbb{Z}_6 . That is, θ^{-1} is a bijection and $\theta^{-1}((a, b) +_{2,3} (c, d)) = \theta^{-1}((a, b)) +_6 \theta^{-1}((c, d))$ for all $(a, b), (c, d)$ in $\mathbb{Z}_2 \times \mathbb{Z}_3$. Let's check the equation in one case. Does $\theta^{-1}((0, 1) +_{2,3} (1, 2))$ equal $\theta^{-1}((0, 1)) +_6 \theta^{-1}((1, 2))$? I.e., does $\theta^{-1}((1, 0))$ equal $\theta^{-1}((0, 1)) +_6 \theta^{-1}((1, 2))$? I.e., does 3 equal $4 +_6 5$? It does.

The Chinese Remainder Theorem can help us solve the problem of finding an n such that $n \% 5 = 3$ and $n \% 7 = 5$. But first, some general background.

Recall that if f is an isomorphism from some group G_1 to another group G_2 , we have $f(a * b) = f(a) * f(b)$ for all a, b in G_1 (where the $*$ on the left side of the equation is the group operation in G_1 and the $*$ on the right side of the equation is the group operation in G_2). Likewise we have $f(a * b * c) = f(a) * f(b) * f(c)$ for all a, b, c in G_1 . Letting $a = b = c$ we have $f(a^2) = (f(a))^2$ and $f(a^3) = (f(a))^3$ and more generally $f(a^n) = (f(a))^n$ for all integers n . In situations where $*$ is written as $+$ (as is the case for the Chinese Remainder Theorem), it's customary to write a^n as na (or sometimes $n \cdot a$), so the formula $f(a^n) = (f(a))^n$ gets written as $f(na) = nf(a)$, meaning that $f(a + a + \dots + a) = f(a) + f(a) + \dots + f(a)$, where the $+$ on the left side is the group operation in G_1 , the $+$ on the right side is the group operation in G_2 , and there are n terms in both the sum $a + a + \dots + a$ and the sum $f(a) + f(a) + \dots + f(a)$.

Enough background; now let's apply it to a specific problem. Say we want to find an n in \mathbb{Z}_{35} satisfying $n \% 5 = 3$ and $n \% 7 = 5$. Since the isomorphism θ from \mathbb{Z}_{35} to $\mathbb{Z}_5 \times \mathbb{Z}_7$ is given by $\theta(n) = (n \% 5, n \% 7)$, all we need to do is compute $\theta^{-1}((3, 5))$. Since θ^{-1} is an isomorphism, it satisfies $\theta^{-1}(a + b) = \theta^{-1}(a) + \theta^{-1}(b)$ for all a, b . In our case, taking $a = (3, 0)$ and $b = (0, 5)$, we get $\theta^{-1}((3, 5)) = \theta^{-1}((3, 0)) + \theta^{-1}((0, 5))$. Since $(3, 0)$ can be written as $3(1, 0)$, the formula from the preceding paragraph tells us that $\theta^{-1}((3, 0)) = \theta^{-1}(3(1, 0)) = 3\theta^{-1}((1, 0))$. Likewise $\theta^{-1}((0, 5)) = \theta^{-1}(5(0, 1)) = 5\theta^{-1}((0, 1))$.

The preceding paragraph tells us that the answer to our original problem ("Find n such that $n \% 5 = 3$ and $n \% 7 = 5$ ") can be reduced to the problem of computing the element $3\theta^{-1}((1, 0)) + 5\theta^{-1}((0, 1))$ in the group \mathbb{Z}_{35} . So if we already know that $\theta^{-1}((1, 0)) = 21$ and $\theta^{-1}((0, 1)) = 15$, we get $3 \cdot \theta^{-1}((1, 0)) + 5 \cdot \theta^{-1}((0, 1)) = 3 \cdot 21 + 5 \cdot 15$. In ordinary arithmetic $3 \cdot 21 + 5 \cdot 15$ equals $63 + 75 = 138$, and $138 \% 35 = 33$, so 33 is our final answer (and we can readily check it: $33 \% 5 = 33 - 30 = 3$ and $33 \% 7 = 33 - 28 = 5$).