Chinese Remainder Theorem

The Chinese Remainder Theorem says that if $n_1, n_2, \ldots, n_k$ are pairwise relatively prime then the system of k –equations

$$x \equiv a_1 \bmod n_1$$
$$x \equiv a_1 \bmod n_2$$
$$\ldots$$
$$x \equiv a_k \bmod n_k$$

has for any choice of k –many integers a_i some solution x and any two solutions x and y are congruent $\bmod n = n_1 \cdot n_2 \cdot \ldots \cdot n_k$.

The uniqueness claim for solutions x and y is quite easy to see: If we have that $x \equiv a_i \bmod n_i, y \equiv a_i \bmod n_i$ then $x - y \equiv 0 \bmod n_i$ That is $n_i | x - y, i = 1, \ldots k.$ Because the n_i are pairwise relatively prime, we get $n | x - y$ which is $x \equiv y \bmod n.$

For the existence of some x we try to find x_i such that $x_i \equiv 1 \bmod n_i$ and $x_i \equiv 0 \bmod n_j$, for $i \neq j.$ Then we put

$$x = a_1 x_1 + a_2 x_2 + \ldots + a_k x_k$$

Then

$x = (a_1 x_1 + a_2 x_2 + \ldots + a_k x_k) \bmod n_1 = a_1 x_1 \bmod n_1 = a_1 \bmod n_1, \ldots, x = (a_1 x_1 + a_2 x_2 + \ldots + a_k x_k$

That is, x is a solution of the given congruence system. In order to find the x_i for the relatively prime n_i we use that

$$(n_i, Ni) = 1 \text{ where } N_i = n/n_i$$

For example $N_1 = n_2 \cdot \ldots n_k.$ Thus we can find u_1 and v_1 such that $u_1 n_1 + v_1 N_1 = 1.$ Therefore $u_1 n_1 + v_1 N_1 \equiv 1 \bmod n_1.$ We set $x_1 = v_1 N_1.$ We similarly find $x_i = v_i N_i, i = 1, \ldots, k.$

Example: Solve

$$x \equiv 2 \bmod 3$$
$$x \equiv 4 \bmod 5$$
$$x \equiv 3 \bmod 7$$

We have $n_1 = 3, N_1 = 5 \cdot 7 = 35; n_2 = 5, N_2 = 3 \cdot 7 = 21; n_3 = 7, N_3 = 3 \cdot 5 = 15$ and

$$1 = 12 \cdot 3 - 1 \cdot (5 \cdot 7)$$
$$1 = (-4) \cdot 5 + 1 \cdot (3 \cdot 7)$$
$$1 = (-2) \cdot 7 + 1 \cdot (3 \cdot 5)$$

this gives us

$$x_1 = -35$$
$$x_2 = 21$$
$$x_3 = 15$$

and

$$x = 2 \cdot (-35) + 4 \cdot 21 + 3 \cdot 15 = 59$$

$x = 59$ is indeed a solution. But so is $y = 59 + 105 = 164$ and the general solution is $59 + k \cdot 105, k \in \mathbb{Z}$

The Chinese Remainder Theorem is a more concrete version of the theorem that a direct product of finitely many finite cyclic groups is cyclic, in case that the orders are relatively prime. If each G_i is cyclic, $G_i =< g_i >$ then the direct product G of the G_i is cyclic and generated by $g = (g_1, g_2, \ldots, g_k)$ in case that $o(g_i)$ and $o(g_j)$ are relatively prime for $i \neq j$. In particular, let $G_i = \mathbb{Z}_{n_i}$, where the n_i are relatively prime, then

$$G = \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \ldots \times \mathbb{Z}_{n_k} =< ([1]_{n_1}, [1]_{n_2}, \ldots, [1]_{n_k}) >$$

and therefore one has for every element $g = ([a_1]_{n_1}, [a_2]_{n_2}, \ldots, [a_{n_k}])$ in G some x such that

$$([a_1]_{n_1}, [a_2]_{n_2}, \ldots, [a_k]_{n_k}) = x.([1]_{n_1}, [1]_{n_2}, \ldots, [1]_{n_k})$$

which is $[a_1]_{n_1} = [x]_{n_1}, [a_2]_{n_2} = [x]_{n_2}, \ldots, [a_k]_{n_k} = [x]_{n_k}$ which is the same as $a_1 = x \bmod n_1, a_2 = x \bmod n_2, \ldots, a_k = x \bmod n_k$. And that is just the Chinese Remainder Theorem.