2.2. **Chinese remainder theorem.** Sometimes we need to solve a system of congruence equations. The main result for this type of problems is the Chinese remainder theorem. We will continue to work in $\mathbb{Z}$ but this theorem is valid in more general situations; see Proposition 2.17 (2013) or Theorem 2.24 (2014) in Algebra 2B for two other versions.

Theorem 2.12. *Suppose that $m_1, m_2, \cdots, m_k$ are pairwise coprime (i.e. $\mathrm{hcf}(m_i, m_j) = 1$ for $i \neq j$) non-zero integers and $m = m_1 m_2 \cdots m_k$. Then the system of congruence equations*

$$\begin{aligned} x &\equiv b_1 \pmod{m_1}, \\ x &\equiv b_2 \pmod{m_2}, \\ &\cdots, \\ x &\equiv b_k \pmod{m_k}. \end{aligned}$$

has a solution, which is unique modulo m.

Proof. We prove it by induction on k. For $k = 1$ there is nothing to prove.

For $k = 2$, an integer solution to $x \equiv b_1 \pmod{m_1}$ is of the form $x = m_1 q + b_1$. So we need to have $m_1 q + b_1 \equiv b_2 \pmod{m_2}$, or $m_1 q \equiv b_2 - b_1 \pmod{m_2}$. Since $\mathrm{hcf}(m_1, m_2) = 1$, by Proposition 2.5, it has a unique solution for q, say $q \equiv q_0 \pmod{m_2}$. Or equivalently, $q = m_2 r + q_0$ for any $r \in \mathbb{Z}$. Hence $x = m_1 m_2 r + (m_1 q_0 + b_1)$ for any $r \in \mathbb{Z}$, which is the unique solution for x modulo $m = m_1 m_2$.

For general k, suppose we have proved the result for $k - 1$. That is, the first $k - 1$ congruence equations have a unique common solution $x \equiv s \pmod{m'}$ for some s, where $m' = m_1 m_2 \cdots m_{k-1}$. Then the problem reduces to a system of two congruences

$$\begin{aligned} x &\equiv s \pmod{m'}, \\ x &\equiv b_k \pmod{m_k}. \end{aligned}$$

By the case for $k = 2$ above, there is a unique solution for x modulo $m = m' m_k$. This finishes the induction. □

To use the theorem to make explicit computations, we just need to follow the proof. We illustrate the idea using the following example.

Example 2.13. Consider the system

$$\begin{aligned} x &\equiv 31 \pmod{41}, \\ x &\equiv 59 \pmod{26}. \end{aligned}$$

From the first equation we can write $x = 41q + 31$. We plug it into the second equation and get $41q + 31 \equiv 59 \pmod{26}$. By removing multiples of 26 we reduce it to $15q \equiv 2$

(mod 26). By Euclidean algorithm, we have $\text{hcf}(15, 26) = 1$ and $15 \times 7 - 26 \times 4 = 1$, which implies $q \equiv 14 \pmod{26}$ is the unique solution for q. If we write $q = 26r + 14$, then $x = 41 \times 26r + (14 \times 41 + 31)$, i.e. $x \equiv 605 \pmod{1066}$.

Remark 2.14. We explain what to do in slightly more complicated situations.

(1) If there are more than two equations in the system, we need to find the common solution to the first two equations, then combine the result with the third equation to find a solution to all three equations, etc. This procedure is reflected by the inductive step in the proof.

(2) If the equations in the system are not in the form of $x \equiv b_i \pmod{m_i}$, we need to solve (at least) one equation before using substitution. See Example 2.15.

(3) In case the m_i's are not pairwise coprime, Theorem 2.12 does not apply any more. Therefore the existence and uniqueness of solutions may not hold. However the substitution method can still be used to solve the system. See Example 2.15.

Example 2.15. Consider the system

$$\begin{aligned} 5x &\equiv 7 \pmod{12}, \\ 7x &\equiv 1 \pmod{10}. \end{aligned}$$

Notice that the coefficients in front of x are not 1. Moreover 12 and 10 are not coprime. We can nevertheless solve it. Using the method in Example 2.7 we find the solution to the first equation $x \equiv 11 \pmod{12}$. Then we write $x = 12q + 11$ and substitute x in the second equation. We get $7(12q + 11) \equiv 1 \pmod{10}$, or $84q \equiv -76 \pmod{10}$. Using the method in Example 2.7 again, we remove multiples of 10 on both sides and cancel the common factor 2 to reduce the equation to $2q \equiv 2 \pmod{5}$, whose solution is $q \equiv 1 \pmod{5}$. Write $q = 5r + 1$ to get $x = 12(5r + 1) + 11 = 60r + 23$. Hence the solution to the original system is $x \equiv 23 \pmod{60}$.

We wish to interpret the Chinese remainder theorem in the language of rings. We need to recall the definition for the direct product of rings; see Definition on Page 27 (2013) or Definition 2.22 (2014) in Algebra 2B.

Definition 2.16. Let $R_1, R_2, \cdots, R_n$ be commutative rings with 1. The *direct product* is the ring

$$R_1 \times R_2 \times \cdots \times R_n = \big\{(a_1, a_2, \cdots, a_n) \mid a_i \in R_i \text{ for each } i\big\},$$

in which addition and multiplication are given component-wise by

$$\begin{aligned} (a_1, a_2, \cdots, a_n) + (b_1, b_2, \cdots, b_n) &= (a_1 + b_1, a_2 + b_2, \cdots, a_n + b_n), \\ (a_1, a_2, \cdots, a_n) \cdot (b_1, b_2, \cdots, b_n) &= (a_1 b_1, a_2 b_2, \cdots, a_n b_n). \end{aligned}$$

Remark 2.17. We make the following observations.

(1) All the algebraic laws hold in $R_1 \times R_2 \times \cdots \times R_n$ since they hold for every component. Clearly the element $(0_{R_1}, 0_{R_2}, \cdots, 0_{R_n})$ is the zero element, and the additive inverse of $(a_1, a_2, \cdots, a_n)$ is $(-a_1, -a_2, \cdots, -a_n)$. The element $(1_{R_1}, 1_{R_2}, \cdots, 1_{R_n})$ is the multiplicative identity. Thus $R_1 \times R_2 \times \cdots \times R_n$ is a commutative ring with 1.

(2) Notice that $(a_1, a_2, \cdots, a_n)$ is a unit in $R_1 \times R_2 \times \cdots \times R_n$ iff a_i is a unit in R_i for each i. We usually denote the group of units of a ring R by R^*, therefore we have

$$(R_1 \times R_2 \times \cdots \times R_n)^* = R_1^* \times R_2^* \times \cdots \times R_n^*.$$

See Remark on Page 27 (2013) or Remark 2.23 (2014) in Algebra 2B.

Now we restate the Chinese remainder theorem as follows:

Corollary 2.18. *Suppose that $m_1, m_2, \cdots, m_k$ are pairwise coprime non-zero integers and $m = m_1 m_2 \cdots m_k$. Then there is a ring isomorphism*

$$\mathbb{Z}_m \cong \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \cdots \times \mathbb{Z}_{m_k}.$$

Proof. For each i there is a natural ring homomorphism $\psi_i : \mathbb{Z} \to \mathbb{Z}_{m_i}$ which maps every integer n to the congruence class modulo m_i containing n. We construct a map $\psi : \mathbb{Z} \to \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \cdots \times \mathbb{Z}_{m_k}$ by $\psi(n) = (\psi_1(n), \psi_2(n), \cdots, \psi(n))$. We can see ψ respects additions and multiplications, because each component ψ_i does. Therefore ψ is a ring homomorphism.

We apply Theorem 2.12. The existence of solutions shows that ψ is surjective; in other words, $\operatorname{im} \psi = \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \cdots \times \mathbb{Z}_{m_k}$. The uniqueness of solutions modulo m shows that $\ker \psi = (m)$. By the fundamental isomorphism theorem of rings (Theorem 1.8 (2013) or Theorem 2.13 (2014) in Algebra 2B), ψ induces a ring isomorphism $\mathbb{Z}/(m) \cong \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \cdots \times \mathbb{Z}_{m_k}$. By Proposition 2.3, the left-hand side is precisely $\mathbb{Z}_m$. □

We have the following immediate consequence concerning the groups of units.

Corollary 2.19. *Suppose that $m_1, m_2, \cdots, m_k$ are pairwise coprime non-zero integers and $m = m_1 m_2 \cdots m_k$. Then there is a group isomorphism*

$$\mathbb{Z}_m^* \cong \mathbb{Z}_{m_1}^* \times \mathbb{Z}_{m_2}^* \times \cdots \times \mathbb{Z}_{m_k}^*.$$

Proof. We apply Remark 2.17 and Corollary 2.18 and obtain

$$\mathbb{Z}_m^* \cong (\mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \cdots \times \mathbb{Z}_{m_k})^* = \mathbb{Z}_{m_1}^* \times \mathbb{Z}_{m_2}^* \times \cdots \times \mathbb{Z}_{m_k}^*$$

as desired. □

Remark 2.20. This result is very helpful in studying the group of units in $\mathbb{Z}_m^*$ for an arbitrary positive integer m. More precisely, let $m = 2^a p_1^{a_1} p_2^{a_2} \cdots p_l^{a_l}$ be the prime decomposition of m, where $p_1, p_2, \cdots p_l$ are distinct odd primes. Since $2^a, p_1^{a_1}, p_2^{a_2}, \cdots, p_l^{a_l}$ are pairwise coprime, we get

$$\mathbb{Z}_m^* \cong \mathbb{Z}_{2^a}^* \times \mathbb{Z}_{p_1^{a_1}}^* \times \mathbb{Z}_{p_2^{a_2}}^* \times \cdots \times \mathbb{Z}_{p_l^{a_l}}^*.$$

Therefore, to understand the group structure of $\mathbb{Z}_m^*$ for an arbitrary m, it suffices to understand it for m being powers of primes. This is what we are going to study next.