

**Lemma.** Let  $n_1, n_2, \dots, n_k$  be natural numbers. If  $(n_i, n_j) = 1$  such that  $i \neq j$  and  $1 \leq i, j, \leq k$ , then  $(n_1 n_2 \dots n_{k-1}, n_k) = 1$ .

**Proof.** Let  $k = 3$  be our base case. By Theorem 2.29,  $(n_1 n_2, n_3) = 1$ . Suppose all  $k$  is true where  $1 \leq k \leq t$ . We want to show  $(n_1 n_2 \dots n_t, n_{t+1}) = 1$ . Since we know up to  $t$  is true, by Theorem 2.29,  $(n_1 n_2 \dots n_t, n_{t+1}) = 1$ . Thus, if  $(n_i, n_j) = 1$  such that  $i \neq j$  and  $1 \leq i, j, \leq k$ , then  $(n_1 n_2 \dots n_{k-1}, n_k) = 1$ .  $\square$

**3.29 Theorem.** (Chinese Remainder Theorem). Suppose  $n_1, n_2, \dots, n_L$  are positive integers that are pairwise relatively prime, that is,  $(n_i, n_j) = 1$  for  $i \neq j$ ,  $1 \leq i, j \leq L$ . Then the system of  $L$  congruences

$$\begin{aligned} x &\equiv a_1 \pmod{n_1} \\ x &\equiv a_2 \pmod{n_2} \\ &\vdots \\ x &\equiv a_L \pmod{n_L} \end{aligned}$$

has a unique solution modulo the product  $n_1 n_2 \dots n_L$ .

**Proof.** Let  $L = 2$ . Consider this the base case. Thus,

$$\begin{aligned} x &\equiv a_1 \pmod{n_1} \\ x &\equiv a_2 \pmod{n_2}. \end{aligned}$$

Since  $(n_1, n_2) = 1$ , by Theorem 3.28,  $x \equiv x' \pmod{n_1 n_2}$ . Thus, the base case is true. Suppose this is true for all  $L$  where  $1 \leq L \leq K$ . By induction, we want to show

$$\begin{aligned} x &\equiv a_1 \pmod{n_1} \\ x &\equiv a_2 \pmod{n_2} \\ &\vdots \\ x &\equiv a_L \pmod{n_K} \\ x &\equiv a_L \pmod{n_{K+1}} \end{aligned}$$

also has a unique solution modulo the product  $n_1n_2\dots n_Kn_{K+1}$ . Thus, the system of congruences is

$$\begin{aligned} x &\equiv a_1 \pmod{n_1} \\ x &\equiv a_2 \pmod{n_2} \\ &\vdots \\ x &\equiv a_K \pmod{n_K} \\ x &\equiv a_{K+1} \pmod{n_{K+1}}. \end{aligned}$$

By our induction hypothesis and Theorem 3.28, we know up to  $K$  is  $x \equiv x' \pmod{n_1n_2\dots n_K}$ . Thus,

$$\begin{aligned} x &\equiv x' \pmod{n_1n_2\dots n_K} \\ x &\equiv a_{K+1} \pmod{n_{K+1}}. \end{aligned}$$

By Theorem 3.28, since  $(n_1n_2\dots n_K, n_{K+1}) = 1$  by the Lemma and Theorem 2.29, and solution  $x$  satisfies

$$x \equiv x'' \pmod{n_1n_2\dots n_Kn_{K+1}},$$

for  $x'' \in \mathbb{Z}$ . Thus, the system of  $L$  congruences has a unique solution modulo the product  $n_1n_2\dots n_L$ .  $\square$