

We claim that

$$x = x_1y_1 + x_2y_2 + \cdots + x_ny_n$$

works. Indeed, using the above congruences, for  $i = 2, \dots, n$ , we get

$$x \equiv x_1y_1 + x_i \pmod{\mathfrak{a}_i}, \quad (*)$$

but since  $\mathfrak{a}_2 \cdots \mathfrak{a}_n \subseteq \mathfrak{a}_i$  for  $i = 2, \dots, n$  and  $y_1 \equiv 0 \pmod{\mathfrak{a}_2 \cdots \mathfrak{a}_n}$ , we have

$$x_1y_1 \equiv 0 \pmod{\mathfrak{a}_i}, \quad i = 2, \dots, n$$

and equation  $(*)$  reduces to

$$x \equiv x_i \pmod{\mathfrak{a}_i}, \quad i = 2, \dots, n.$$

For  $i = 1$ , we get

$$x \equiv x_1 \pmod{\mathfrak{a}_1},$$

therefore

$$x \equiv x_i \pmod{\mathfrak{a}_i}, \quad i = 1, \dots, n.$$

proving surjectivity. □

The classical version of the Chinese Remainder Theorem is the case where  $A = \mathbb{Z}$  and where the ideals  $\mathfrak{a}_i$  are defined by  $n$  pairwise relatively prime integers  $m_1, \dots, m_n$ . By the Bezout identity, since  $m_i$  and  $m_j$  are relatively prime whenever  $i \neq j$ , there exist some  $u_i, u_j \in \mathbb{Z}$  such that  $u_im_i + u_jm_j = 1$ , and so  $m_i\mathbb{Z} + m_j\mathbb{Z} = \mathbb{Z}$ . In this case, we get an isomorphism

$$\mathbb{Z}/(m_1 \cdots m_n)\mathbb{Z} \approx \prod_{i=1}^n \mathbb{Z}/m_i\mathbb{Z}.$$

In particular, if  $m$  is an integer greater than 1 and

$$m = \prod_i p_i^{r_i}$$

is its factorization into prime factors, then

$$\mathbb{Z}/m\mathbb{Z} \approx \prod_i \mathbb{Z}/p_i^{r_i}\mathbb{Z}.$$

In the previous situation where the integers  $m_1, \dots, m_n$  are pairwise relatively prime, if we write  $m = m_1 \cdots m_n$  and  $m'_i = m/m_i$  for  $i = 1, \dots, n$ , then  $m_i$  and  $m'_i$  are relatively prime, and so  $m'_i$  has an inverse modulo  $m_i$ . If  $t_i$  is such an inverse, so that

$$m'_i t_i \equiv 1 \pmod{m_i},$$