For all $\alpha, \beta \in \mathbb{Z}_n$ and $\kappa, \ell \in \mathbb{Z}$, we have the identities:

$$k(\ell\alpha) = (k\ell)\alpha = \ell(k\alpha), (k+\ell)\alpha = k\alpha + \ell\alpha, k(\alpha+\beta) = k\alpha + k\beta,$$
$$(k\alpha)\beta = k(\alpha\beta) = \alpha(k\beta).$$

Analogously, for $\alpha_1, ..., \alpha_\kappa \in \mathbb{Z}_n$, we may write their product as $\Pi_{i=1}^{k}\alpha_i$. By convention, this product is [1] when $\kappa = 0$ it is easy to see that if all of the $\alpha_i's$ belong to $\mathbb{Z}_n^*$, then so does their product, and in particular, $(\Pi^k i = 1\alpha_i)^{-1} = \Pi^{ki=1}\alpha_i^{-1}$; that is, the multiplicative inverse of the product is the product of the multiplicative

inverses. In the special case where all the $\alpha_i's$ have the same value `$\alpha$` , we define $\alpha^\kappa := \Pi_{i=1}^{\kappa}\alpha$; thus $\alpha^0 = [1], \alpha^1 = \alpha, \alpha^2 = \alpha\alpha, \alpha^3 = \alpha\alpha\alpha$, and so on. If a $\alpha \in \mathbb{Z}_n^*$, then the multiplicative inverse of α^k is $(a^{-1)\kappa}$, which we may also write as $\alpha^- k$; for example, $\alpha^{-2} = \alpha^{-1}\alpha^{-1} = (\alpha\alpha)^{-1}$. Therefore, when $\alpha \in \mathbb{Z}_n^*$, the notation α^k is defined for all integers `$\kappa$`.

$$(\alpha^\ell)^k = \alpha^{k\ell} = (\alpha^{k)\ell}, \alpha^{k+\ell} = \alpha^k\alpha^\ell, (\alpha\beta)^k = \alpha^{k\beta k}. \quad (2.7)$$

If $\alpha, \beta \in \mathbb{Z}_n^*$, the identities in (2.7) hold for all `$\kappa$` , `$\ell$` ,$\in \mathbb{Z}$.
For all $\alpha_1, ..., \alpha_\kappa, \beta_1, ..., \beta_\ell \in \mathbb{Z}_n$, he distributive property implies that

$$(\alpha_1 + ... + \alpha_k)(\beta_1 + ... + \beta_\ell) = \sum_{1 \le i \le k 1 \le j \le \ell} \alpha_i\beta_j.$$

One last notational convention. As already mentioned, when the modulus n is clear from context, we usually write $[\alpha]$ instead of $[\alpha]_n$ although we want to maintain a clear distinction between integers and their residue classes, occasionally even the notation $[\alpha]$ is not only redundant, but distracting; in such situations, we may simply write α instead of $[\alpha]$ For example, for every $\alpha \in \mathbb{Z}_n$, we have the

identity $(\alpha + [1]_n)(\alpha - [1]_n) = \alpha^2 - [1]_n$, which we may write more simply as $(\alpha + [1])(\alpha - [1]) = \alpha^2 - [1]$, or even more simply, and hopefully more clearly, as $(\alpha + 1)(\alpha - 1) = \alpha^2 - 1$. Here, the only reasonable interpretation of the symbol 1 is [1], and so there can be no confusion.

In summary, algebraic expressions involving residue classes may be manipulated in much the same way as expressions involving ordinary numbers. Extra complications arise only because when n is composite, some non-zero elements of $\mathbb{Z}_n$ do not have multiplicative inverses, and the usual cancellation law does not apply for such elements. In general, one has a choice between

working with congruences modulo n, or with the algebraic structure $\mathbb{Z}_n$; ultimately, the choice is one of taste and convenience, and it depends on what

one prefers to treat as first class objects: integers and congruence relations, or elements of $\mathbb{Z}_n$.

An alternative, and somewhat more concrete, approach to constructing $\mathbb{Z}_n$ is to directly define it as the set of n symbols $[0], [1], ..., [n-1]$, with addition and multiplication defined as

$$[a] + [b] := [(a + b) \text{mod } n], \;\; [a].[b] := [(a.b) \text{ mod } n],$$

for $a, b \in 0, ..., n-1$. Such a definition is equivalent to the one we have given here. One should keep this alternative characterization of $\mathbb{Z}_n$ in mind; however, we prefer the characterization in terms of residue classes, as it is mathematically more elegant, and is usually more convenient to work with.

We close this section with a reinterpretation of the Chinese remainder theorem(Theorem 2.6) in terms of residue classes.

Theorem 2.8 (Chinese remainder map). Let $n_{i_{i=1}}^{\kappa}$ be a pairwise relatively prime family of positive integers, and let $n := \Pi_{i=1}^{\kappa} n_i$. Define the map

$$\begin{array}{rl} \theta : & \mathbb{Z}_n \to \mathbb{Z}_{n_1} x ... x \mathbb{Z}_{n_k} \\ & [a]_n \mapsto ([a]_{n1}, ..., [a]_{nk}). \end{array}$$

i) The definition of `$\theta$` is unambiguous.

ii) θ is bijective.

iii) For all $\alpha, \beta \in \mathbb{Z}_n$, if $\theta(\alpha) = (\alpha_1, ..., \alpha_\kappa)$ and $\theta(\beta) = (\beta_1, ..., \beta_\kappa)$, then:

a) $\theta(\alpha + \beta) = (\alpha_1 + \beta_1, ...,)\alpha_k + \beta_k)$;

b) $\theta(-a) = (-\alpha_1, ..., -\alpha_k)$;

c) $\theta(\alpha\beta) = (\alpha_1\beta_1, ..., \alpha_k\beta_k)$

d) $a \in \mathbb{Z}_n^*$ if and only if $a_i \in \mathbb{Z}_{n_i}^*$ for $i = 1, ..., k$,in which case $\theta(a^-1) = (a_1^{-1}, ..., a_k^{-1})$.

Proof. For (i), note that $a \equiv a' (\text{mod } n) \text{implies} a \equiv a' (mod n_i) \text{for} i = 1, ..., \kappa$, and so the definition of θ is unambiguous (it does not depend on the choice of a). (ii) follows directly from the statement of the Chinese remainder theorem.

For (iii), let $a = [a]_n and \beta = [b]_n$, so that for $i = 1, .., k$, we have $a_i = [a]_{ni}$ and $\beta_i = [b]_{ni}$. Then we have.

$$\theta(\alpha+\beta)=\theta([\alpha+b]_n)=([a+b]_{n1},...,[a+b]_{n\kappa})=(\alpha_1+\beta_1,...,\alpha_\kappa+\beta_\kappa),$$
$$\theta(-\alpha)=\theta([-\alpha]_n)=([-\alpha]_{n1},...,[-\alpha]_{nk})=(-\alpha_1,...,\alpha_\kappa),and$$
$$\theta(\alpha\beta)=\theta([\alpha b]_n)=([\alpha b]_{n1},...,[\alpha b]_{n\kappa})=(\alpha_1\beta_1,...,\alpha_\kappa\beta_\kappa)$$

That proves parts (a), (b), and (c). For part (d), we have

$$\alpha\in\mathbb{Z}_n^*\iff gcd(a,n)=1$$
$$\iff gcd(a,n_i)=1 for i=1,...,\kappa$$
$$\iff \alpha_i\in\mathbb{Z}_{ni}^* for i=1,...,k.$$

Moreover, if $\alpha\in\mathbb{Z}_n^*$ and $\beta=a^{-1}$, then

$$(\alpha_1\beta_1,...,\alpha_\kappa\beta_\kappa)=\theta(\alpha\beta)=\theta([1]_n)=([1]_{n1},...,[1]_{n1},...,[1]_{nk}),$$

and so for $i=1,...,\kappa$, we have $\alpha_i\beta_i=[1]_{ni}$, which is to say $\beta_i=\alpha_i^{-1}$.

Theorem 2.8 is very powerful conceptually, and is an indispensable tool in many situations. It says that if we want to understand what happens when we add or multiply $\alpha,\beta\in\mathbb{Z}_n$, it suffices to understand what happens when we add or multiply their components $\alpha,\beta_i\in\mathbb{Z}_{ni}$, Typically, we choose $n_1,...,n_\kappa$ to be primes or prime powers, which usually simplifies the analysis. We shall see many applications of this idea throughout the text.

EXERCISE 2.19. Let $\theta:\mathbb{Z}_n\longrightarrow\mathbb{Z}_{n1}\times....\times\mathbb{Z}_{nk}$ be as in Theorem 2.8, and suppose that $\theta(\alpha)=(\alpha_1,...,\alpha_\kappa)$. Show that for every non-negative integer m, we have $\theta(\alpha^m)=(\alpha_1^m,...,\alpha_k^m)$. Moreover, if $\alpha\in\mathbb{Z}_1^*$ show that this identity holds for all integers m.

EXERCISE 2.20 Let p be an odd prime. Show That $\sum_{\beta\in\mathbb{Z}_p^*}\beta=0$.

EXERCISE 2.21. Let p be an odd prime. Show that the numerator of $\sum_{i=1}^{p-1}1/i$ is divisible by p.

EXERCISE 2.22. Suppose n is square-free (see Exercise 1.15), and let $\alpha,\beta,\gamma\in\mathbb{Z}_n$. Show that $\alpha^2\beta=a^2\gamma$ implies $\alpha\beta=\alpha\gamma$

2.6 Eulers phi function

Eulers phi function (also called **Eulers totient function**) is defined for all positive integers n as

$$\varphi(n):=|\mathbb{Z}_n^*|.$$

Equivalently, $\varphi(n)$ is equal to the number of integers between 0 and $n-1$ that are relatively prime to n. For example, $\varphi(1)=1,\varphi(2)=1,\varphi(3)=2$, and $\varphi(4)=2$. Using the Chinese remainder theorem, more specifically Theorem 2.8, it is easy to get a nice formula for $\varphi(n)$ in terms of the prime factorization of n, as we establish in the following sequence of theorems.