

1.4 Integers Modulo n

The ideas in this section allow us to work with equations instead of congruences, provided we think in terms of equivalence classes. To be more precise, any linear congruence of the form

$$ax \equiv b \pmod{n}$$

can be viewed as an equation in \mathbf{Z}_n , written

$$[a]_n[x]_n = [b]_n.$$

This gives you one more way to view problems involving congruences. Sometimes it helps to have various ways to think about a problem, and it is worthwhile to learn all of the approaches, so that you can easily shift back and forth between them, and choose whichever approach is the most convenient. For example, trying to divide by a in the congruence $ax \equiv b \pmod{n}$ can get you into trouble unless $\gcd(a, n) = 1$. Instead of thinking in terms of division, it is probably better to think of multiplying both sides of the equation $[a]_n[x]_n = [b]_n$ by $[a]_n^{-1}$, provided $[a]_n^{-1}$ exists.

It is well worth your time to learn about the sets \mathbf{Z}_n and \mathbf{Z}_n^\times . They will provide an important source of examples in Chapter 3, when we begin studying groups.

The exercises for Section 1.4 of the text contain several definitions for elements of \mathbf{Z}_n . If $(a, n) = 1$, then the smallest positive integer k such that $a^k \equiv 1 \pmod{n}$ is called the *multiplicative order* of $[a]$ in \mathbf{Z}_n^\times . The set \mathbf{Z}_n^\times is said to be *cyclic* if it contains an element of multiplicative order $\varphi(n)$. Since $|\mathbf{Z}_n^\times| = \varphi(n)$, this is equivalent to saying that \mathbf{Z}_n^\times is cyclic if has an element $[a]$ such that each element of \mathbf{Z}_n^\times is equal to some power of $[a]$. Finally, the element $[a] \in \mathbf{Z}_n$ is said to be *idempotent* if $[a]^2 = [a]$, and *nilpotent* if $[a]^k = [0]$ for some k .

SOLVED PROBLEMS: §1.4

30. Find the multiplicative inverse of each nonzero element of \mathbf{Z}_7 .
31. Find the multiplicative inverse of each nonzero element of \mathbf{Z}_{13} .
32. Find $[91]_{501}^{-1}$, if possible (in \mathbf{Z}_{501}^\times).
33. Find $[3379]_{4061}^{-1}$, if possible (in \mathbf{Z}_{4061}^\times).
34. In \mathbf{Z}_{20} : find all units (list the multiplicative inverse of each); find all idempotent elements; find all nilpotent elements.
35. In \mathbf{Z}_{24} : find all units (list the multiplicative inverse of each); find all idempotent elements; find all nilpotent elements.
36. Show that \mathbf{Z}_{17}^\times is cyclic.

37. Show that \mathbf{Z}_{35}^\times is not cyclic but that each element has the form $[8]_{35}^i[-4]_{35}^j$, for some positive integers i, j .
38. Solve the equation $[x]_{11}^2 + [x]_{11} - [6]_{11} = [0]_{11}$.
39. Let n be a positive integer, and let $a \in \mathbf{Z}$ with $\gcd(a, n) = 1$. Prove that if k is the smallest positive integer for which $a^k \equiv 1 \pmod{n}$, then $k \mid \varphi(n)$.
40. Prove that $[a]_n$ is a nilpotent element of \mathbf{Z}_n if and only if each prime divisor of n is a divisor of a .