

Consider the modular number system  $\mathbb{Z}_9$

1. Write the complete  $9 \times 9$  addition and multiplication tables. For example, we have  $\bar{6} + \bar{7} = \bar{13} = \bar{4}$ , so in the addition table, the entry in the  $\bar{6}$  row and  $\bar{7}$  column should be  $\bar{4}$ . Hint: For simplicity, don't write the lines over the numbers in the table: just keep in mind that all the entries are classes in  $\mathbb{Z}_9$ , so that everything is modulo 9.

2. Looking at the multiplication table, determine which elements  $\bar{a} \in \mathbb{Z}_9$  have inverses  $\bar{a}^{-1}$ .

3. Determine which elements have square roots. That is, for which  $\bar{a} \in \mathbb{Z}_9$  is there some  $\bar{b} \in \mathbb{Z}_9$  with  $\bar{b}^2 = \bar{a}$ ?

4. Use the quadratic formula to solve the equation  $x^2 + \bar{3}x + \bar{5} = \bar{0}$  for  $x \in \mathbb{Z}_9$ . (For this part of the problem, see the discussion below.)

**Modular algebra.** Since  $\mathbb{Z}_p$  (for  $p$  a prime) obeys all the usual axioms of addition and multiplication, almost everything we know about algebra carries over to  $\mathbb{Z}_p$ , provided we remember that  $\bar{p} = \bar{0}$ .

For example, the quadratic formula gives the solutions to the equation  $ax^2 + bx + c = 0$ :

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

Now, if we want to solve an equation like:

$$x^2 + \bar{2}x + \bar{3} = \bar{0} \quad \text{for } x \in \mathbb{Z}_{11},$$

we apply the quadratic formula to the number system  $\mathbb{Z}_{11}$ . We need the square root of  $b^2 - 4ac = \bar{4} - \bar{12} = \bar{-8} = \bar{3}$ , which by definition is some  $y \in \mathbb{Z}_{11}$  with  $y^2 = \bar{3}$ . By trial and error we find  $\bar{5}^2 = \bar{25} = \bar{3}$ , so we take  $y = \bar{5}$ . Also, dividing by  $2a = \bar{2}$  means multiplying by  $\bar{2}^{-1} = \bar{6}$ . Thus we get:

$$x = (-b \pm y)(2a)^{-1} = (-\bar{2} \pm \bar{5})(\bar{6}) = \bar{18}, \bar{-42} = \bar{7}, \bar{2}.$$

Check: for  $x = \bar{7}$ , we have:  $(\bar{7})^2 + \bar{2}(\bar{7}) + \bar{3} = \bar{66} = \bar{0}$ , and similarly for  $x = \bar{2}$ .