

8 1. (a) Apply the Euclidean algorithm to find the greatest common divisor of 18 and 50. (The work shown must illustrate the Euclidean algorithm, and not some other method.)

8 (b) Where  $d = (18, 50)$ , calculate a solution in the integers to the equation  $18x + 50y = d$ .

4 (c) Find a solution to the equation  $[18]X = [d]$  in the ring  $\mathbb{Z}_{50}$ .

$$\begin{aligned}
 (a) \quad 50 &= 2(18) + 14 \\
 &= 3(18) - 4 \\
 18 &= 4(4) + 2 \\
 4 &= 2(2) + 0. \quad \therefore (18, 50) = \textcircled{2}.
 \end{aligned}$$

$$\begin{aligned}
 (b) \quad 2 &= 18 - 4(4) \\
 &\quad \nearrow 4 = 3(18) - 50
 \end{aligned}$$

$$\begin{aligned}
 2 &= 18 - 4[3(18) - 50] \\
 &= -11(18) + 4(50).
 \end{aligned}$$

$x = -11, y = 4$  is one solution.

Another one is  $x = 14, y = -5$ .

$$(c) \quad -11(18) + 4(50) = 2$$

$X = [-11] = \textcircled{[39]}$  is a solution.

$X = [14]$  is also a solution.

- 8 2. (a) Calculate  $3^{406}$  modulo 5. (That is, find the integer  $r$  with  $0 \leq r < 5$  that is congruent to  $3^{406}$ .) Suggestion: Start with  $3^4$ .
- 6 (b) Find all the units in  $\mathbb{Z}_{24}$ .
- 6 (c) For half of the units in  $\mathbb{Z}_{24}$ , find their inverses. (No fancy method is needed here.)

$$(a) \quad 3^4 = 81 \equiv 1.$$

$$3^{406} = (3^4)^{101} \cdot 3^2 \equiv 1 \cdot 9 \equiv \textcircled{4}.$$

(b)  $[a]$  is a unit when  $(a, 24) = 1$ .

There are eight units:

$$[1], [5], [7], [11],$$

$$[13] = [-11], [17] = [-7], [19] = [-5], [23] = [-1].$$

(c)

$$1^2 = 1, \quad 5^2 = 25 \equiv 1, \quad 7^2 = 49 \equiv 1, \quad 11^2 = 121 \equiv 1,$$

$$(-11)^2 = 121 \equiv 1, \quad (-7)^2 = 49 \equiv 1, \quad (-5)^2 = 25 \equiv 1,$$

$$(-1)^2 = 1.$$

Conclusion  $x^{-1} = x$  for each of the eight units  $x$  in  $\mathbb{Z}_{24}$ .

- 10 3. (a) How many different divisors does 300 have in  $\mathbb{Z}$ ? 36 (Show your work.)
- 5 (b) Is there a *smallest* natural number  $n$  such that some finite field has exactly size  $n$ ? Yes Support your answer.
- 5 (c) Is there a *largest* natural number  $n$  such that some finite field has exactly size  $n$ ? No Support your answer.

$$(a) 300 = 2^2 \cdot 3 \cdot 5^2$$

$$\text{divisor: } \pm 2^{[0 \text{ or } 1 \text{ or } 2]} \cdot 3^{[0 \text{ or } 1]} \cdot 5^{[0 \text{ or } 1 \text{ or } 2]}$$

We can make a divisor in  $2 \times 3 \times 2 \times 3 = 36$  ways.

(b)  $n = 2$ . On the one hand, there is a field of size 2, viz.  $\mathbb{F}_2$ . On the other hand, there is no field of smaller size, because  $0 \neq 1$  in a field.

(c)  $\mathbb{F}_p$  is a field for each prime  $p$ , and there are arbitrarily large primes.

4. Show that addition in  $\mathbb{Z}_m$  is well defined, by doing the following.

(a) Show that if  $a \equiv a' \pmod{m}$  and  $b \equiv b' \pmod{m}$  then  $a + b \equiv a' + b' \pmod{m}$ .

(b) Show that if in  $\mathbb{Z}_m$  we have  $[a] = [a']$  and  $[b] = [b']$ , then  $[a + b] = [a' + b']$ .

(a) We have  $a - a' = m\ell$  and  $b - b' = m\ell$   
for some  $m, \ell$ .

$$\begin{aligned} (a + b) - (a' + b') &= (a - a') + (b - b') \\ &= m\ell + m\ell = m(\ell + \ell). \end{aligned}$$

$$\text{So } a + b \equiv a' + b' \pmod{m}.$$

$$(b) [a] = [a'] \Rightarrow a \equiv a' \pmod{m}$$

$$[b] = [b'] \Rightarrow b \equiv b' \pmod{m}$$

Together, we have from part (a) that

$$a + b \equiv a' + b' \pmod{m}.$$

$$\therefore [a + b] = [a' + b'].$$

See page 74 and page 97.

5. Assume that  $R$  with  $+$ ,  $\cdot$ ,  $0_R$ , and  $1_R$  is a commutative ring with identity.
- 10 (a) Prove that additive inverses are unique. That is, show that if both  $x + y = 0_R$  and  $x + z = 0_R$ , then  $y = z$ . (This is the fact need<sup>ed</sup> to justify the definition of  $-x$ , so the notation " $-x$ " cannot be used here.)
- 10 (b) Assume that  $a$  is an element of  $R$  that is not  $0_R$  and is not a zero divisor. Show that the following cancellation law holds: whenever  $a \cdot x = a \cdot y$ , then  $x = y$ .

(a) Look at  $z + x + y$ .

~~On~~ On the one hand,  $z + x + y =$   
 $(z + x) + y = (x + z) + y = 0 + y = y.$

On the other hand,  $z + x + y =$   
 $z + (x + y) = z + 0 = z.$

Conclusion:  $y = z$ . See page 129.

(b) Given  $ax = ay$ . Using ring properties gives

$$\begin{array}{l} \text{not } 0 \\ \text{not a zero divisor} \end{array} \quad \begin{array}{c} \uparrow \\ a(x - y) = 0 \end{array}$$

$$\therefore x - y = 0,$$

so  $x = y$ . See page 135.