

**1:** Solve each of the following linear congruences.

- (a)  $5x \equiv 4 \pmod{7}$
- (b)  $40x \equiv 15 \pmod{65}$
- (c)  $391x \equiv 119 \pmod{1003}$

**2:** (a) Find  $[12]^{-1}$  in  $\mathbf{Z}_{29}$ .

(b) Solve  $[34]x = [18]$  in  $\mathbf{Z}_{46}$ .

(c) In  $\mathbf{Z}_{20}$ , solve the pair of simultaneous equations

$$[7]x + [12]y = [6]$$

$$[6]x + [11]y = [13]$$

**3:** (a) Find the inverse of every invertible element in  $\mathbf{Z}_{15}$ .

(b) With the help of the following list of powers of 5 mod 23, solve  $[11]x^{18} = [15]$  in  $\mathbf{Z}_{23}$ .

$k$	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
$5^k$	1	5	2	10	4	20	8	17	16	11	9	22	18	21	13	19	3	15	6	7	12	14

**4:** (a) Find  $17^{458} \pmod{13}$ .

(b) Find  $47^{38^{54}} \pmod{11}$ .

(c) Find  $\sum_{k=1}^{300} k^k \pmod{7}$ .

**5:** For this problem, you may find it useful to read some of sections 9.1 and 9.9 in the text. In particular in section 9.1, have a look at the example involving long division in  $\mathbf{Z}_5$  on page 231, and see the Remainder Theorem 9.12 and the Factor Theorem 9.14 on page 232, and in section 9.9, look at example 9.92 on page 260. It is also worth noticing that Theorem 9.17 in section 9.1 does not always hold for polynomials over  $\mathbf{Z}_n$ .

(a) Solve  $x^2 + 3x + 2 \equiv 0 \pmod{6}$ , then find two different ways to factor the polynomial  $f(x) = x^2 + [3]x + [2]$  over  $\mathbf{Z}_6$ .

(b) Solve  $x^2 + 2x + 26 \equiv 0 \pmod{125}$ , then find two different ways to factor the polynomial  $f(x) = x^2 + [2]x + [26]$  over  $\mathbf{Z}_{125}$ .