1. Assignment due January 23, 2003:
§ 0.1: 1, 2, 3, 4, 6, 7
§ 0.2: 1 (d, f), 3, 4, 8

2. Assignment due January 30, 2003:
§ 0.3: 3, 4, 5, 6, 7, 8, 11, 15(c)
§ 1.1: 1, 2, 5, 6, 9, 11, 14, 21, 25, 29, 30

EXERCISES § 0.1

In Exercises 1 to 4 let $\mathcal{A}$ be the set of 2×2 matrices with real number entries. Recall that matrix multiplication is defined by

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} p & q \\ r & s \end{pmatrix} = \begin{pmatrix} ap+br & aq+bs \\ cp+dr & cq+ds \end{pmatrix} \quad .$$

Let

$$M = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

and let

$$\mathcal{B} = \{X \in \mathcal{A} \mid MX = XM\}.$$

1. Determine which of the following elements of $\mathcal{A}$ lie in $\mathcal{B}$:

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

2. Prove that if $P, Q \in \mathcal{B}$, then $P + Q \in \mathcal{B}$ (where $+$ denotes the usual sum of two matrices).

3. Prove that if $P, Q \in \mathcal{B}$, then $P \cdot Q \in \mathcal{B}$ (where $\cdot$ denotes the usual product of two matrices).

4. Find conditions on p, q, r, s which determine precisely when $\begin{pmatrix} p & q \\ r & s \end{pmatrix} \in \mathcal{B}$.

6. Determine whether the function $f : \mathbb{R}^+ \to \mathbb{Z}$ defined by mapping a real number r to the first digit to the right of the decimal point in a decimal expansion of r is well defined.

7. Let $f : A \to B$ be a surjective map of sets. Prove that the relation

$$a \sim b \text{ if and only if } f(a) = f(b)$$

is an equivalence relation whose equivalence classes are the fibers of f.

EXERCISES § 0.2

1. For each of the following pairs of integers a and b, determine their greatest common divisor, their least common multiple, and write their greatest common divisor in the form $ax + by$ for some integers x and y.
(a) $a = 20$, $b = 13$.
(b) $a = 69$, $b = 372$.
(c) $a = 792$, $b = 275$.
(d) $a = 11391$, $b = 5673$.
(e) $a = 1761$, $b = 1567$.
(f) $a = 507885$, $b = 60808$.

3. Prove that if n is composite then there are integers a and b such that n divides ab but n does not divide either a or b.

4. Let a, b and N be fixed integers with a and b nonzero and let $d = (a, b)$ be the greatest common divisor of a and b. Suppose x_0 and y_0 are particular solutions to $ax + by = N$ (i.e., $ax_0 + by_0 = N$). Prove for any integer t that the integers

$$x = x_0 + \frac{b}{d}t \quad \text{and} \quad y = y_0 - \frac{a}{d}t$$

are also solutions to $ax + by = N$ (this is in fact the general solution).

8. Let p be a prime, $n \in \mathbb{Z}^+$. Find a formula for the largest power of p which divides $n! = n(n-1)(n-2)\ldots 2 \cdot 1$ (it involves the greatest integer function).

EXERCISES § 0.3

3. Prove that if $a = a_n 10^n + a_{n-1}10^{n-1} + \cdots + a_1 10 + a_0$ is any positive integer then $a \equiv a_n + a_{n-1} + \cdots + a_1 + a_0 \pmod 9$ (note that this is the usual arithmetic rule that the remainder after division by 9 is the same as the sum of the decimal digits mod 9 – in particular an integer is divisible by 9 if and only if the sum of its digits is divisible by 9) [note that $10 \equiv 1 \pmod 9$].

4. Compute the remainder when 37^{100} is divided by 29.

5. Compute the last two digits of 9^{1500}.

6. Prove that the squares of the elements in $\mathbb{Z}/4\mathbb{Z}$ are just $\bar{0}$ and $\bar{1}$.

7. Prove for any integers a and b that $a^2 + b^2$ never leaves a remainder of 3 when divided by 4 (use the previous exercise).

8. Prove that the equation $a^2 + b^2 = 3c^2$ has no solutions in nonzero integers a, b and c. [Consider the equation mod 4 as in the previous two exercises and show that a, b and c would all have to be divisible by 2. Then each of a^2, b^2 and c^2 has a factor of 4 and by dividing through by 4 show that there would be a smaller set of solutions to the original equation. Iterate to reach a contradiction.]

11. Prove that if $\bar{a}, \bar{b} \in (\mathbb{Z}/n\mathbb{Z})^\times$, then $\bar{a} \cdot \bar{b} \in (\mathbb{Z}/n\mathbb{Z})^\times$.

15. For each of the following pairs of integers a and n, show that a is relatively prime to n and determine the multiplicative inverse of $\bar{a}$ in $\mathbb{Z}/n\mathbb{Z}$.

(a) $a = 13$, $n = 20$.
(b) $a = 69$, $n = 89$.
(c) $a = 1891$, $n = 3797$.
(d) $a = 6003722857$, $n = 77695236973$. [The Euclidean Algorithm requires only 3 steps for these integers.]

EXERCISES § 1.1

Let G be a group.

1. Determine which of the following binary operations are associative:

(a) the operation $\star$ on $\mathbb{Z}$ defined by $a \star b = a - b$
(b) the operation $\star$ on $\mathbb{R}$ defined by $a \star b = a + b + ab$
(c) the operation $\star$ on $\mathbb{Q}$ defined by $a \star b = \dfrac{a+b}{5}$

(d) the operation $\star$ on $\mathbb{Z} \times \mathbb{Z}$ defined by $(a, b) \star (c, d) = (ad + bc, bd)$

(e) the operation $\star$ on $\mathbb{Q} - \{0\}$ defined by $a \star b = \dfrac{a}{b}$.

2. Decide which of the binary operations in the preceding exercise are commutative.

5. Prove for all $n > 1$ that $\mathbb{Z}/n\mathbb{Z}$ is not a group under multiplication of residue classes.

6. Determine which of the following sets are groups under addition:

(a) the set of rational numbers (including 0 = 0/1) in lowest terms whose denominators are odd

(b) the set of rational numbers (including 0 = 0/1) in lowest terms whose denominators are even

(c) the set of rational numbers of absolute value < 1

(d) the set of rational numbers of absolute value ≥ 1 together with 0

(e) the set of rational numbers with denominators equal to 1 or 2

(f) the set of rational numbers with denominators equal to 1, 2 or 3.

9. Let $G = \{a + b\sqrt{2} \in \mathbb{R} \mid a, b \in \mathbb{Q}\}$.

(a) Prove that G is a group under addition.

(b) Prove that the nonzero elements of G are a group under multiplication. [“Rationalize the denominators” to find multiplicative inverses.]

11. Find the orders of each element of the additive group $\mathbb{Z}/12\mathbb{Z}$.

14. Find the orders of the following elements of the multiplicative group $(\mathbb{Z}/36\mathbb{Z})^\times$: $\overline{1}$, $\overline{-1}$, $\overline{5}$, $\overline{13}$, $\overline{-13}$, $\overline{17}$.

21. Let G be a finite group and let x be an element of G of order n. Prove that if n is odd, then $x = (x^2)^k$ for some k.

25. Prove that if $x^2 = 1$ for all $x \in G$ then G is abelian.

29. Prove that $A \times B$ is an abelian group if and only if both A and B are abelian.

30. Prove that the elements $(a, 1)$ and $(1, b)$ of $A \times B$ commute and deduce that the order of (a, b) is the least common multiple of $|a|$ and $|b|$.