Section 0.2

Exercise (0.2.1c). For the following pair of integers $a = 792$ and $b = 275$, 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.

Solution: Computing the gcd of a, b by the Euclidean Algorithm, as stated by Property 6 in Section 0.2, we get,

$$\begin{aligned}
792 &= (2)275 + 242,\\
275 &= (1)242 + 33,\\
242 &= (7)33 + 11,\\
33 &= (3)11.
\end{aligned}$$

Thus the gcd $= 11$. Computing the lcm by solving (gcd)(lcm) $= ab$ as stated by Property 4 in Section 0.2 we get,

$$\text{lcm} = \frac{ab}{\text{gcd}} = \frac{(792)(275)}{(11)} = 19800.$$

Expressing the gcd in the form of $ax + by$ with $x, y \in \mathbb{Z}$, by repeated substitution in each step of the Euclidean Algorithm we get,

$$\begin{aligned}
11 &= 242 - (7)33\\
&= [792 - (2)275] - (7)[275 - 242]\\
&= [792 - (2)275] - (7)[275 - [792 - (2)275]]\\
&= [792 - (2)275] - [(7)275 - (7)792 + (14)275]\\
&= 792 - (2)275 - (7)275 + (7)792 - (14)275\\
&= (8)792 - (23)275\\
&= 792(8) + 275(-23).
\end{aligned}$$

$\square$

Exercise (0.2.3). 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.

Proof: Suppose that n is composite. By definition of composite there exists some positive divisors $a, b \neq 1, n$ such that $ab = n(1)$. Clearly $n \mid ab$. Note that $b = n(\frac{1}{a})$ and $a = n(\frac{1}{b})$. Since $\frac{1}{a}, \frac{1}{b}$ are $\notin \mathbb{Z}$ we have shown that $n \nmid a, b$. $\square$

Exercise (0.2.5). Determine the value of $\varphi(n)$ for each integer $n \geq 30$ where φ denotes the Euler φ-function.

Solution: Let p be prime and for all $a \geq 1$ we know that,

$$\varphi(p^a) = p^{a-1}(p-1),$$

following formula discussed in Example 10 of Section .2. We also know that a, b are relatively prime the φ-function is multiplicative, so

$$\varphi(ab) = \varphi(a)\varphi(b)$$

Computing the values we get,

$$\varphi(1) = 1$$
$$\varphi(2) = 2^{1-1}(2-1) = 1$$
$$\varphi(3) = 3^{1-1}(3-1) = 2$$
$$\varphi(4) = 2^{2-1}(2-1) = 2$$
$$\varphi(5) = 5^{1-1}(5-1) = 4$$
$$\varphi(6) = \varphi(2)\varphi(3) = 2$$
$$\varphi(7) = 7^{1-1}(7-1) = 6$$
$$\varphi(8) = 2^{3-1}(2-1) = 4$$
$$\varphi(9) = 3^{2-1}(3-1) = 6$$
$$\varphi(10) = \varphi(5)\varphi(2) = 4$$
$$\varphi(11) = 11^{1-1}(11-1) = 10$$
$$\varphi(12) = \varphi(4)\varphi(3) = 4$$
$$\varphi(13) = 13^{1-1}(13-1) = 12$$
$$\varphi(14) = \varphi(7)\varphi(2) = 6$$
$$\varphi(15) = \varphi(3)\varphi(5) = 8$$
$$\varphi(16) = 2^{4-1}(2-1) = 8$$
$$\varphi(17) = 17^{1-1}(17-1) = 16$$
$$\varphi(18) = \varphi(9)\varphi(2) = 6$$
$$\varphi(19) = 19^{1-1}(19-1) = 18$$
$$\varphi(20) = \varphi(5)\varphi(4) = 8$$
$$\varphi(21) = \varphi(7)\varphi(3) = 12$$
$$\varphi(22) = \varphi(11)\varphi(2) = 10$$
$$\varphi(23) = 23^{1-1}(23-1) = 22$$
$$\varphi(24) = \varphi(8)\varphi(3) = 8$$
$$\varphi(25) = 5^{2-1}(5-1) = 20$$
$$\varphi(26) = \varphi(13)\varphi(2) = 12$$
$$\varphi(27) = 3^{3-1}(3-1) = 18$$
$$\varphi(28) = \varphi(7)\varphi(4) = 12$$
$$\varphi(29) = 29^{1-1}(29-1) = 28$$
$$\varphi(30) = \varphi(10)\varphi(3) = 8$$

$\square$

Exercise (0.2.10). Prove for any given positive integer N there exist only finitely many integers n with $\varphi(n) = N$ where φ denotes Euler's φ-function. Conclude in particular that $\varphi(n)$ tends to infinity as n tends to infinity.

Proof: Let $N \in \mathbb{Z}^+$, and $X = \{n \in \mathbb{Z} : \varphi(n) = N\}$. By the Fundamental Theorem of Arithmetic, $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_s^{\alpha_s}$ for primes p_i and $\alpha_i \in \mathbb{Z}^+$. Consider prime p, the largest of primes p_i. It follows that,

$$N = \varphi(n) = \prod_{i=1}^{s} p_i^{\alpha_i - 1}(p_i - 1) \geq (p-1).$$

Therefore for all follows that $p_i \leq p \leq N+1$.

Note that

$$N = \varphi(n) = \prod_{i=1}^{s} p_i^{\alpha_i - 1}(p_i - 1) \geq \prod_{i=1}^{s} p_i^{\alpha_i - 1} \geq \prod_{i=1}^{s} 2^{\alpha_i - 1}.$$

Consider α, the largest element in the set of α_i. It follows that,

$$N \geq \prod_{i=1}^{s} 2^{\alpha_i - 1} \geq 2^{\alpha - 1}.$$

Therefore $\alpha_1 \leq \alpha \leq \lceil \log_2(N) + 1 \rceil$. Since p_i is finite, and s_i is finite, and whose elements are bounded above by some function of N then the set,

$$A = \{x = \prod_{i=1}^{s} q_i^{\beta_i} : q_i \in p_i, \beta_i \in \alpha_i\}$$

is finite with $a \in A$ bounded above by some function of N. Note that X is a subset of A and therefore X is finite, and for all $n \in X$, n is bounded above by some function of N. Thus as n tends to infinity $\varphi(n)$ also tends to infinity. □

Exercise (0.2.11). Prove that if d divides n then $\varphi(d)$ divides $\varphi(n)$ where φ denotes Euler's φ-function

Proof: Suppose $d, n \in \mathbb{Z}^+$ such that $d \mid n$. By definition $n = d(i)$ for some $i \in \mathbb{Z}^+$. By the Fundamental Theorem of Arithmetic, let d, n be expressed a products of prime powers for sufficiently large s and $\alpha_i, \beta_i \geq 0$, $d = \prod_{i=1}^{s} p_i^{\alpha_i}$, and $n = \prod_{i=1}^{s} p_i^{\beta_1}$. Since $n = d(i)$ we know that $0 \leq \alpha_i \leq \beta_i$. Now consider $\varphi(n)$,

$$\varphi(n) = \prod_{i=1}^{s} p_i^{\beta_i - 1}(p_i - 1) = \left(\prod_{i=1}^{s} p_i^{\beta_i - \alpha_i - 1}\right)(j)\left(\prod_{i=1}^{s} p_i^{\alpha_i - 1}(p_i - 1)\right)$$

where $j \in \mathbb{Z}$ is any unnecessary product of $(p_i - 1)$ that is left over. Note that for $k \in \mathbb{Z}$,

$$\varphi(n) = (\prod_{i=1}^{s} p_i^{\beta_i - \alpha_i - 1} j)\varphi(d) = k\varphi(d).$$

Thus $\varphi(d)$ divides $\varphi(n)$. □

Section 0.3

Exercise (0.3.4). Compute the remainder when 37^{100} is divided by 29.

Solution: Consider group $\mathbb{Z}/29\mathbb{Z}$ under multiplication. We know from Theorem 3 that we can multiply congruences. Computing a few powers to construct $37^{1}00$ we get,

$$37 \equiv 8 \mod 29$$

$$37^2 \equiv 8^2 = 64 \equiv 6 \mod 29$$

$$37^4 \equiv 6^2 = 36 \equiv 7 \mod 29$$

$$37^8 \equiv 7^2 = 49 \equiv 20 \mod 29$$

$$37^{16} \equiv 20^2 = 400 \equiv 23 \mod 29$$

$$37^{32} \equiv 23^2 = 529 \equiv 7 \mod 29$$

Using these congruences we can compute the following,

$$37^{100} = (37^{32})^3 37^4 \equiv 7^4 = 2401 \equiv 23 \mod 29$$

So the remainder is 23. □

Exercise (0.3.5). Compute the last two digits of 9^{1500}.

Solution: To compute the last two digits of 9^{1500} we want to find the remainder after division by 100. Similarly to exercise 4 we will compute the remainder of a few powers of 9 to eventually multiply the congruences and compute 9^{1500}.

$$9^2 = 81 \mod 100$$

$$9^4 = 81^2 = 6561 \equiv 61 \mod 100$$

$$9^8 = 61^2 = 3721 \equiv 21 \mod 100$$

$$9^{16} = 21^2 = 441 \equiv 41 \mod 100$$

$$9^{32} = 41^2 = 1681 \equiv 81 \mod 29$$

Having computed a reminder of 81, we know that each subsequent square of 9^{32} will follow the same pattern in the remainder as we previously computed. Therefore, $9^{64} \equiv 61 \mod 100$, $9^{128} \equiv 21 \mod 100$, $9^{256} \equiv 41 \mod 100$, $9^{512} \equiv 81 \mod 100$, and $9^{1024} \equiv 61 \mod 100$. Finally we can compute the remainder of 9^{1500},

$$\begin{aligned} 9^{1500} &= 9^{1024+256+128+64+16+8+4} \\ &= 9^{1024}9^{256}9^{128}9^{64}9^{16}9^{8}9^{4} \\ &\equiv 61^{3}41^{2}21^{2} \\ &\equiv 1 \mod 100 \end{aligned}$$

Therefore the last two digits of 9^{1500} are '01'. □

Exercise (0.3.9). Prove that the square of any odd integer always leaves a remainder of 1 when divided by 8.

Proof: Suppose $n \in \mathbb{Z}$ is odd. By the definition, for some $i \in \mathbb{Z}$, $n = 2(i) + 1$. Consider n^2,

$$n^2 = (2(i) + 1)(2(i) + 1) = 4(i)^2 + 4(i) + 1 = 4i(i + 1) + 1.$$

Note that when i is odd, $i + 1$ must be even and vice versa. Therefore we can always factor out a 2 from the product $i(i + 1)$ giving us for some $j \in \mathbb{Z}$,

$$sn^2 = 8(j) + 1.$$

□

Exercise (0.3.13). Let $n \in \mathbb{Z}$, $n > 1$, and let $a \in \mathbb{Z}$ with $1 \geq a \geq n$. Prove if a and n are relatively prime then there is an integer c such that $ac \equiv 1 \mod n$ [use the fact that the g.c.d. of two integers is a $\mathbb{Z}$- linear combination of the integers].

Proof: Let $n \in \mathbb{Z}$, $n > 1$, and $a \in \mathbb{Z}$ with $1 \geq a \geq n$ such that a and n are relatively prime. Recall Property 7 of the integers, since $1 \geq a \geq n$ we can write the g.c.d. of a, b as a linear combination of $x, y \in \mathbb{Z}$. Note that since a and n are relatively prime we know that their g.c.d. is 1 thus,

$$1 = ax + ny,$$

$$(1 - ax) = ny.$$

Therefore $n \mid (1 - ax)$ and by definition $ax \equiv 1 \mod n$. $\square$

Section 1.1

Exercise (1.1.8). Let $G = \{z \in \mathbb{C} | z^n = 1 \text{ for some } n \in \mathbb{Z}^+\}$

a. Prove that G is a group under multiplication (called the group of roots of unity in $\mathbb{C}$).

Proof: Suppose $G = \{z \in \mathbb{C} | z^n = 1 \text{ for some } n \in \mathbb{Z}^+\}$. Let $a, b \in G$ such that $a^j = b^k = 1$ for some $i, j \in \mathbb{Z}^+$. Note that G is closed under multiplication, $ab \in \mathbb{C}$ and

$$(ab)^{jk} = a^{jk}b^{jk} = (a^j)^k(b^k)^j = 1.$$

Recall that the set of $\mathbb{C}$ is associative under multiplication, so G must also be associative under multiplication. Now note that $1 \in \mathbb{C}$ and $1^1 = 1$ so $1 \in G$ and therefore under multiplication, G has an identity element. Let $z \in G$, and consider $\frac{1}{z} \in \mathbb{C}$. Note that,

$$\left(\frac{1}{z}\right)^n = \frac{1}{z^n} = \frac{1}{1} = 1$$

Therefore $\frac{1}{z} \in G$ and thus every element in G has an inverse under multiplication. Thus G is a group. $\square$

b. Prove that G is not a group under addition.

Proof: In the previous problem we showed that $1 \in G$. Note that $1 + 1 = 2$ and $2 \notin G$ since $2^n = 1$ for $n \in \mathbb{Z}^+$ has no solution. Thus G is not closed under addition. $\square$

Exercise (1.1.11). Find the orders of each element of the additive group $\mathbb{Z}/12\mathbb{Z}$.

Solution: Recall that, $ZZ/12\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}, \overline{7}, \overline{8}, \overline{9}, \overline{10}, \overline{11}\}$ and that in the additive group, 0 is the identity. Also recall that the order of $x \in \mathbb{Z}/12\mathbb{Z}$ is the smallest $n \in \mathbb{Z}^+$ such that $x^n = 0$, and we denote the order of x with $|x| = n$. Note that under an additive group exponentiation by n is equivalent to multiplication. Thus,

$$\overline{0}(1) = \overline{0} \qquad \overline{6}(2) = \overline{0}$$
$$\overline{1}(12) = \overline{0} \qquad \overline{7}(12) = \overline{0}$$
$$\overline{2}(6) = \overline{0} \qquad \overline{8}(3) = \overline{0}$$
$$\overline{3}(4) = \overline{0} \qquad \overline{9}(4) = \overline{0}$$
$$\overline{4}(3) = \overline{0} \qquad \overline{10}(6) = \overline{0}$$
$$\overline{5}(12) = \overline{0} \qquad \overline{11}(12) = \overline{0}$$

Thus the orders of the element $x \in \mathbb{Z}/12\mathbb{Z}$

x	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$	$\overline{8}$	$\overline{9}$	$\overline{10}$	$\overline{11}$
$\|x\|$	1	12	6	4	3	12	2	12	3	4	6	12

□

Exercise (1.1.13). Find the orders of the following elements of the additive group $\mathbb{Z}/36\mathbb{Z}$: $\overline{1}, \overline{2}, \overline{6}, \overline{9}, \overline{10}, \overline{12}, \overline{-1}, \overline{-10}, \overline{-18}$.

Solution: Similarly to the last problem, we can find the order of $x \in \mathbb{Z}/36\mathbb{Z}$ by finding the smallest $n \in \mathbb{Z}^+$ such that $x^n = 0$, and again with an additive group exponentiation by n is equivalent to multiplication. Doing so we get the following,

$$\overline{1}(36) = \overline{0}$$
$$\overline{2}(18) = \overline{0}$$
$$\overline{6}(6) = \overline{0}$$
$$\overline{9}(4) = \overline{0}$$
$$\overline{10}(18) = \overline{0}$$
$$\overline{12}(3) = \overline{0}$$
$$\overline{-1}(36) = \overline{0}$$
$$\overline{-10}(18) = \overline{0}$$
$$\overline{-18}(2) = \overline{0}$$

Thus we get the following orders,

x	$\overline{1}$	$\overline{2}$	$\overline{6}$	$\overline{9}$	$\overline{10}$	$\overline{12}$	$\overline{-1}$	$\overline{-10}$	$\overline{-18}$
$\|x\|$	36	18	6	4	18	3	36	18	2

□

Exercise. 1.1.21 Let G be a finite group and let x be an element of G order n. Prove that if n is odd, then $x = (x^2)^k$ for some k.

Proof: Let be G a finite group with $x \in G$ such that $|x| = n$ and n is an odd integer. Note that since x has order n, $x^n = \epsilon$ where ϵ is the identity element in G. Note that n is odd and therefore, $n = 2i + 1$ for some $i \in \mathbb{Z}$. Thus,

$$x = \epsilon x = (x^n)x = (x^{2i+1})x = x^{2i+2} = (x^2)^{(i+1)}.$$

□

Exercise. 1.1.22 If x and g are element of the group G, prove that $|x| = |g^{-1}xg|$. Deduce that $|ab| = |ba|$ for all $a, b \in G$.

Proof: Suppose $x, g \in G$. Let $|x| = n$. Consider $(g^{-1}xg)^n$,

$$(g^{-1}xg)^n = (g^{-1})x^n g = g^{-1}g = \epsilon.$$

Thus $|g^{-1}xg| \leq n = |x|$. Now let $|g^{-1}xg| = i$ and consider x^i,

$$x^i = \epsilon x^i \epsilon = gg^{-1}x^i gg^{-1} = g(g^{-1}x^i g)g^{-1}.$$

Note that $(g^{-1}x^ig) = (g^{-1}xg)^i$. Since $|g^{-1}xg| = i$ we get, $(g^{-1}x^ig) = (g^{-1}xg)^i = \epsilon$ and by substitution,

$$x^i = g(g^{-1}x^ig)g^{-1} = g\epsilon g^{-1} = \epsilon.$$

Thus $|x| \leq i = |g^{-1}xg|$. Since we have shown that, $|g^{-1}xg| \leq |x|$ and $|x| \leq |g^{-1}xg|$ it is the case that $|x| = |g^{-1}xg|$.

We can deduce $|ab| = |ba|$ for all $a, b \in G$ with the equality $|x| = |g^{-1}xg|$ by letting $x = ab$ and $g = b^{-1}$. Doing so we get the following,

$$|ab| = |b(ab)b^{-1}| = |ba(bb^{-1})| = |ba|.$$

$\square$

Exercise (1.1.25). Prove that if $x^2 = \epsilon$ for all $x \in G$ then G is abelian.

Proof: Suppose $x^2 = \epsilon$ for all $x \in G$. With some algebra we get,

$$x^2 = \epsilon,$$

$$x^2(x^{-1}) = \epsilon(x^{-1}),$$

$$x = x^{-1}.$$

Now consider some $a, b \in G$, and with (4) of Proposition 1 we can consider the following,

$$ab = (ab)^{-1} = b^{-1}a^{-1} = ba.$$

Thus G is abelian. $\square$

Exercise (1.1.31). Prove that any finite group G of even order contains an element of order 2.[Let $t(G)$ be the set $\{g \in G | g \neq g^{-1}\}$. Show that $t(G)$ has an even number of element and every nonidentity element of $G - t(G)$ has order 2.]

Proof: Suppose a finite group G with $|G| = n$ such that n is even. Now consider $G - \{\epsilon\}$ and note it has odd order. Therefore for some $i \in \mathbb{Z}^+$, $|G - \{\epsilon\}| = 2i + 1$. Consider that to be a group each element in G must have a unique inverse. With at most i pairs of distinct elements and $2i+1$ total elements by the Pigeon Hole Principle there must exists some $x \in |G - \{\epsilon\}|$ such that $x = x^{-1}$. Therefore,

$$x = x^{-1},$$

$$x(x) = x^{-1}(x),$$

$$x^2 = \epsilon.$$

Thus $|x| = 2$. □

Section 1.2

Exercise (1.2.1a). Compute the order of each of the elements in $D_{2(3)}$. [D_{2n} has the usual presentation $D_{2n} = \{r, s | r^n = s^2 = 1, rs = sr^{-1}\}$.]

Solution: With our presentation, $D_{2(3)} = \{1, r, r^2, s, sr, sr^2\}$, as described in Section 1.2. Trivially $|1| = 1$. From our presentation we know $r^3 = 1$. Note that $r^2 \neq 1$ since it would imply that $r^3 = rr^2 = r$ and not $r = 1$, thus $|r| = 3$. Geometrically this makes sense, since it corresponds to 3 rotations of $(2pi/3)$ on the regular 3-gon and $(3)(2pi/3) \equiv 0 \mod (2\pi)$.

Note that $(r^2)^2 = r^4 = r^3 r = r \neq 1$ and $(r^2)^3 = r^6 = r^3 r^3 = 1$, thus $|r^2| = 3$. Geometrically this corresponds to 3 rotations of $(4\pi/3)$ on the regular 3-gon and $(3)(4pi/3) \equiv 0 \mod (2\pi)$.

From our presentation we know that $s^2 = 1$ so $|s| = 2$.

Consider that $(sr)^2 = srsr = s(rs)r$ and by our presentation we know that $rs = sr^{-1}$ so by substitution we get $(sr)^2 = ssr^{-1}r = s^2 = 1$, thus $|(sr)^2| = 2$.

Similarly $(sr^2)^2 = sr^2sr^2 = sr(rs)rr = sr(sr^{-1})rr = srsr = 1$. Below is a table summarizing our results,

x	1	r	r^2	s	sr	sr^2
$\lvert x\rvert$	1	3	3	2	2	2

□

Exercise (1.2.2). Use the generators and relations above to show that if x is any element of D_{2n}, which is not a power of r, then $rx = xr^{-1}$.

Proof: Suppose $x \in D_{2n}$ such that x is not a power of r. By definition $x = sr^i$ such that $0 \geq i \geq n-1$. Substituting $rs = sr^{-1}$ from our presentation we get,

$$rx = r(sr^i) = (rs)r^i = s(r^{-1}r^i).$$

Note that rotations r in D_{2n} commute so therefore,

$$rx = s(r^{-1}r^i) = (sr^i)r^{-1} = xr^{-1}.$$

□

Section 1.3

Exercise (1.3.4b). Compute the order of the elements in S_4.

Solution: First recall from the end of Section 1.3 that that the order of a permutation is the l.c.m of the lengths of the cycles in it's cycle decomposition. Now we can compute the order of each permutation in S_4,

Permutation (σ)	$\lvert\sigma\rvert$
(1)	1
(12)	2
(13)	2
(14)	2
(23)	2
(24)	2
(34)	2

Permutation (σ)	$\lvert\sigma\rvert$
(123)	3
(124)	3
(132)	3
(134)	3
(142)	3
(143)	3
(234)	3
(243)	3

Permutation (σ)	$\lvert\sigma\rvert$
(1234)	4
(1243)	4
(1324)	4
(1342)	4
(1423)	4
(1432)	4

Permutation (σ)	$\lvert\sigma\rvert$
(12)(34)	2
(13)(24)	2
(14)(23)	2

$\square$

Exercise (1.3.5). Find the order of $\sigma = (1128104)(213)(5117)(69)$.

Solution: Recall from the end of section 1.3 that that the order of a permutation is the l.c.m of the lengths of the cycles in it's cycle decomposition. Note that the lengths of the cycles in $\sigma = (1128104)(213)(5117)(69)$ are 5,2,3,2 respectively. Note that the lengths are all prime numbers so the l.c.m. and therefore $|\sigma|$ is simply the product of $5 * 3 * 2 = 30$. $\square$

Exercise (1.3.10). Prove that if σ is the m-cycle $(a_1 a_2 \ldots a_m)$, then for all $i \in [m]$, $\sigma^i(a_k) = a_{k+i}$, where $k + i$ is replaced by its least residue $\mod m$ when $k + 1 > m$. Deduce that $|\sigma| = m$.

Proof: Suppose that $\sigma = (a_1 a_2 \ldots a_m)$ for some $m \in \mathbb{Z}^+$. We will proceed to show for all $\sigma^i(a_k) = a_{k+i}$ by induction on i. Consider the base case $i = 1$. By the definition of $\sigma = (a_1 a_2 \ldots a_m)$ it follows that $\sigma^1(a_k) = a_{k+1}$. Suppose that $\sigma^i(a_k) = a_{k+i}$ hold for some $1 \leq i \leq m - 1$. Note that,

$$\begin{aligned}
\sigma^{i+1}(a_k) &= \sigma(\sigma^i(a_k)) \\
&= \sigma(\sigma^i(a_k)) \\
&= \sigma(a_{k+1}) \\
&= a_{(k+1)+1}
\end{aligned}$$

Thus by induction for all $i \in [m]$, $\sigma^i(a_k) = a_{k+i}$, where $k+i$ is replaced by its least residue $\mod m$ when $k+1 > m$.

Finally, note that for every σ^i where $1 \leq i \leq m-1$, σ^i maps a_k to a_{k+i} and since $k+i \not\equiv kmodn$ we know that $a_k \neq a_{k+i}$. When $i = m$ we get that σ^m maps a_k to a_{k+m} and since $k+m \equiv kmodm$ we know that $a_k = a_{k+m}$. Thus we have shown that $\sigma^m = 1$ and that $|\sigma| = m$. $\square$

Exercise (1.3.15). Prove that the order of an element in S_n equals the least common multiple of the lengths of the cycles in its cycle decomposition.

Proof: Suppose $\sigma \in S_n$ such that σ has the following cycle decomposition with k disjoint cycles,

$$\sigma = s_1 s_2 \dots s_k.$$

Suppose that $|\sigma| = m$, and consider that,

$$(\sigma)^m = (s_1 s_2 \dots s_k)^m.$$

Since disjoint cycles commute we know that,

$$(\sigma)^m = (s_1)^m (s_2)^m \dots (s_k)^m = 1.$$

Therefore it follows that for all $i \in [k]$, $s_i^m = 1$. In Exercise 10 we showed that $s_i^m = 1$ is only possible when m is some multiple of the length of s_1, and therefore it follows that m must be some multiple of the lengths of s_i. Since $|\sigma| = m$ it must be the least common multiple of all the lengths of s_i. $\square$

Exercise (1.3.18). Find all numbers n such that S_5 contains an element of order n.

Solution: Note that for $1 \leq n \leq 5$, S_5 contains an n-cycle. For example

$$1, (12), (123), (1234), (12345).$$

S_5 also contains elements of order 6. For example,

$$(12)(345).$$

Constructing an element with a larger cycle, or different lengths would require $n \geq 7$. $\square$

Section 1.4

Exercise (1.4.3). Show that $\mathbb{GL}_2(\mathbb{F}_2)$ is non-abelian.

Proof: Consider the following $A, B \in \mathbb{GL}_2(\mathbb{F}_2)$,

$$A = \begin{pmatrix} 1 & 2 \\ 0 & 2 \end{pmatrix}, B = \begin{pmatrix} 2 & 4 \\ 0 & 1 \end{pmatrix}.$$

Note that,

$$AB = \begin{bmatrix} 2 & 6 \\ 0 & 2 \end{bmatrix}$$

and,

$$BA = \begin{pmatrix} 2 & 12 \\ 0 & 2 \end{pmatrix}$$

$\square$

Exercise (1.4.10). Let

$$G = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} | a, b, c \in \mathbb{R}, a, c \neq 0 \right\}$$

a. Show G is closed under matrix multiplication.

Proof: Let $A, B \in G$ such that,

$$A = \begin{pmatrix} a_1 & b_1 \\ 0 & c_1 \end{pmatrix}, B = \begin{pmatrix} a_2 & b_2 \\ 0 & c_2 \end{pmatrix}$$

Note that,

$$AB = \begin{pmatrix} a_1 & b_1 \\ 0 & c_1 \end{pmatrix} \begin{pmatrix} a_2 & b_2 \\ 0 & c_2 \end{pmatrix} = \begin{pmatrix} a_1 a_2 & a_1 b_2 + b_1 c_2 \\ 0 & c_1 c_2 \end{pmatrix}.$$

Clearly $a_1a_2, a_1b_2 + b_1c_2, c_1c_2 \in \mathbb{R}$ and $a_1a_2, c_1c_2 \neq 0$ thus $AB \in G$. □

b. Find a matrix inverse of,

$$A = \begin{pmatrix} a & b \\ 0 & c \end{pmatrix}.$$

Proof: Let,

$$A^{-1} = \begin{pmatrix} a^{-1} & -b(a^{-1})(c^{-1}) \\ 0 & c^{-1} \end{pmatrix}.$$

Now consider that AA^{-1}

$$AA^{-1} = \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \begin{pmatrix} a^{-1} & (a^{-1})(-b)(c^{-1}) \\ 0 & c^{-1} \end{pmatrix} = \begin{pmatrix} aa^{-1} & (aa^{-1})(-bc^{-1}) + bc^{-1} \\ 0 & cc^{-1} \end{pmatrix} = I_2$$

□

c Deduce that G is a subgroup of $\mathbb{GL}_2(\mathbb{R})$.

Proof: Solution: Recall that for a $G \leq \mathbb{GL}_2(\mathbb{R}$ it must be the case that G is a non-empty subset of $\mathbb{GL}_2(\mathbb{R}$ and G must be closed under matrix multiplication and inverses. G is clearly a subset of $\mathbb{GL}_2(\mathbb{R})$ as any non-singular upper triangular 2x2 real matrix is also a 2x2 real matrix. We also illustrated that G is closed under matrix multiplication and inverses in the previous parts. Thus $G \leq \mathbb{GL}_2(\mathbb{R}$. □

d Prove that the set of elements of G whose two diagonal entries are equal is also a subgroup of $\mathbb{GL}_2(\mathbb{R})$.

Proof: Let,

$$U = \left\{ \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} | a, b \in \mathbb{R}, a \neq 0 \right\}.$$

Note that for $A, B \in U$,

$$AB = \begin{pmatrix} a_1 & b_1 \\ 0 & a_1 \end{pmatrix} \begin{pmatrix} a_2 & b_2 \\ 0 & a_2 \end{pmatrix} = \begin{pmatrix} a_1a_2 & a_1b_2 + b_1a_2 \\ 0 & a_1a_2 \end{pmatrix}.$$

Thus $AB \in U$ and U is closed under matrix multiplication. Now consider $A, A^{-1} \in U$,

$$AA^{-1} = \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \begin{pmatrix} a^{-1} & -b(a^{-2}) \\ 0 & a^{-1} \end{pmatrix} = \begin{pmatrix} aa^{-1} & -b(a^{-2}a) + b(a^{-1}) \\ 0 & aa^{-1} \end{pmatrix} = I_2$$

Thus U is closed under inverses. Therefore U is a subgroup of $\mathbb{GL}_2(\mathbb{R})$. □

1.5

Exercise (1). Compute the order of each of the elements in $\mathbb{Q}_8$.

Proof: Solution: From the description of $\mathbb{Q}_8$ in Section 1.5 we get the following table of orders,

x	1	-1	i	$-i$	j	$-j$	k	$-k$
$\lvert x\rvert$	1	2	4	4	4	4	4	4

□