MODEL ANSWERS TO THE SECOND HOMEWORK

1.2.1 Let $c = a^{-1} \cdot a$. We compute

$$\begin{aligned} c \cdot c &= (a^{-1} \cdot a) \cdot (a^{-1} \cdot a) \\ &= a^{-1} \cdot (a \cdot a^{-1}) \cdot a \\ &= (a^{-1} \cdot e) \cdot a \\ &= a^{-1} \cdot a \\ &= c. \end{aligned}$$

As $c \in G$ it follows that $c \cdot c^{-1} = e$. Multiplying the equation $c^2 = c$ on the left by c^{-1} we get

$$\begin{aligned} e &= c \cdot c^{-1} \\ &= c^2 \cdot c^{-1} \\ &= c \cdot (c \cdot c^{-1}) \\ &= c \cdot e \\ &= c. \end{aligned}$$

Thus $c = e$. It follows that $a^{-1} \cdot a = e$, so that e is unique. Finally we compute

$$\begin{aligned} e \cdot a &= (a \cdot a^{-1}) \cdot a \\ &= a \cdot (a^{-1} \cdot a) \\ &= a \cdot e \\ &= a. \end{aligned}$$

Thus G is indeed a group.
1.2.4. The even integers are a group. They are closed under addition and inverses. They are not a ring, since 1 is not an even integer. The positive integers is not even a group as it does not contain an identity.
1.2.5. Suppose that we can cancel. Suppose that $ab = 0$ and $a \neq 0$. As $a \cdot 0 = 0$ we have

$$ab = a \cdot 0.$$

Cancelling a we get

$$b = 0.$$

Now suppose that $ab = 0$ implies either that $a = 0$ or $b = 0$.

Suppose that

$$ab = ac$$

and $a \neq 0$. Then

$$\begin{aligned} a(b-c) &= ab - ac \\ &= 0. \end{aligned}$$

As $a \neq 0$, it follows that $b - c = 0$, so that $b = c$.
1.4.10 If

$$a = p_1^{e_1} p_2^{e_2} \dots p_l^{e_l}$$

then the natual number b divides a if it has a prime factorisation of the form

$$b = p_1^{f_1} p_2^{f_2} \dots p_l^{f_l}$$

where $0 \leq f_i \leq e_i$. For each index i there are $e_i + 1$ choices of f_i and so

$$\tau(a) = \prod_{i=1}^{l} (e_i + 1).$$

It is clear that $\tau(a)$ only depends on the set

$$\{\, e_i \,|\, 1 \leq i \leq l \,\}.$$

$\tau(a)$ is odd if and only if all of the exponents e_i are even.
If m and n are coprime then

$$\tau(mn) = \tau(m)\tau(n).$$

Suppose that m and n are coprime. We first check that

$$\sigma(mn) = \sigma(m)\sigma(n).$$

Note that if d divides mn then we can write $d = d_1 d_2$ where d_1 divides m and d_2 divides n. Thus

$$\begin{aligned} \sigma(m)\sigma(n) &= (\sum_{d_1|m} d_1)(\sigma_{d_2|n}) \\ &= \sum_{d_1|m, d_2|n} d_1 d_2 \\ &= \sum_{d|mn} d \\ &= \sigma(mn). \end{aligned}$$

On the other hand, the divisors of p^e are 1, p, …, p^e, so that

$$\sigma(p^e) = 1 + p + p^2 + \dots + p^e.$$

It follows that

$$\sigma(a) = \prod_{i=1}^{l}(1 + p_i + p_i^2 + \cdots + p_i^{e_i}).$$

1.4.13 There are two possible interpretations of this problem. In the first interpretation, k ranges over the non-negative integers and in the second interpretation k ranges over all of the integers. Let the range of k be I (the choice of I only changes the last bit of the problem).
The set

$$S = \{\, 6k + 1 \,|\, k \in I \,\},$$

is closed under multiplication, as

$$\begin{aligned}(6a + 1)(6b + 1) &= 36ab + 6a + 6b + 1 \\ &= 6(6ab + a + b) + 1.\end{aligned}$$

$1 = 6 \cdot 0 + 1 \in S$. S satisfies the cancellation law as the integers satisfy the cancellation law.
We say that $a \in S$ divides $b \in S$ if there an element $c \in S$ such that $b = ac$. We say that $p \in S$ is S-prime if whenever $p = ab$, for a and $b \in$ then either $p = a$ or $p = b$.
Suppose that I is the non-negative integers. Unique factorisation does not hold in this set. Consider the integer

$$5 \cdot 5 \cdot 11 \cdot 11.$$

We can write this as

$$25 \cdot 121.$$

Both 25 and 121 belong to S. 25 is an S-primes, as 5 does not belong to S and 121 is an S-prime as 11 does not belong to S. Similarly we can write the product as

$$55 \cdot 55.$$

55 belongs to S. It is an S-prime as neither 5 nor 11 belong to S.
Thus

$$25 \cdot 121 = 55 \cdot 55,$$

are two distinct ways to write the same element of S as a product of S-primes.
Now suppose that $I = \mathbb{Z}$. Then unique factorisation does hold. Pick $a \in S$. If $a = 1$ then there is nothing to prove. Otherwise a is a product of ordinary primes $q_1, q_2, \ldots, q_k$, except where we allow negative numbers (so that, for example, -2, -3 are considered to be primes). If every $q_i \in S$ then $q_i = p_i$ is an S-prime.

Suppose that $q_i \notin S$. Then $q_i \neq 2$, since then a is even and a does not belong to S. Similarly $q_i \neq 3$. Thus $q_i = 6k + 5$. It follows that

$$\begin{aligned} -q_i &= 6(-k) - 5 \\ &= 6(-k-1) + 1 \in S. \end{aligned}$$

Suppose that $q_j \notin S$ as well. Then we can flip the sign of both q_i and q_j,

$$a = q_1 q_2 \dots q_{i-1}(-q_i)q_{i+1} \dots q_{j-1}(-q_j)q_{j+1} \dots q_k.$$

Continuing in this way, either we write a as a product of S-primes, or exactly one of the primes $q_1, q_2, \dots, q_k$ does not belong to S.
The product b of the other primes does belong to S, since S is closed under multiplication. $-q_i \in S$ so that $-a = (-q_i) \cdot b \in S$. But it is not possible that both a and $-a \in S$.
2.1.1. It is clear that both 4655 and 12075 are divisible by 5. We divide both of these numbers by 5 and calculate the greatest common divisor of what is left. We want to calculate the greatest common divisor of 931 and 2415. It we look for other common low prime factors we see that 7 is a common factor. If we divide through by 7 we have to find the greatest common divisor of 133 and 345.
We first divide 133 into 345. We have

$$345 = 2 \cdot 133 + 79$$

Thus the quotient is 2 and the remainder is 79. Now we divide 79 into 133. We have

$$133 = 1 \cdot 79 + 54.$$

Thus the quotient is 1 and the remainder is 54. Now we divide 54 into 79. We have

$$79 = 1 \cdot 54 + 25.$$

Thus the quotient is 1 and the remainder is 25. Now we divide 25 into 54. We have

$$54 = 2 \cdot 25 + 4.$$

Thus the quotient is 2 and the remainder is 4. Now we divide 4 into 25. We have

$$25 = 6 \cdot 4 + 1.$$

Thus the quotient is 6 and the remainder is 1. Now we divide 1 into 24. We have

$$4 = 4 \cdot 1 + 0.$$

Thus the quotient is 4 and the remainder is 0. Thus the greatest common divisor of 133 and 345 is one. It follows that the greatest common divisor of 4655 and 12075 is 35.

We now write 1 as a linear combination of 133 into 345. We go backwards. From

$$25 = 6 \cdot 4 + 1 \qquad \text{we get} \qquad 1 = 25 - 6 \cdot 4.$$

From

$$54 = 2 \cdot 25 + 4 \qquad \text{we get} \qquad 4 = 54 - 2 \cdot 25.$$

Thus

$$\begin{aligned} 1 &= 25 - 6 \cdot 4 \\ &= 25 - 6 \cdot (54 - 2 \cdot 25) \\ &= 13 \cdot 25 - 6 \cdot 54. \end{aligned}$$

From

$$79 = 1 \cdot 54 + 25 \qquad \text{we get} \qquad 25 = 79 - 1 \cdot 54.$$

Thus

$$\begin{aligned} 1 &= 13 \cdot 25 - 6 \cdot 54 \\ &= 13 \cdot (79 - 1 \cdot 54) - 6 \cdot 54 \\ &= 13 \cdot 79 - 19 \cdot 54. \end{aligned}$$

From

$$133 = 1 \cdot 79 + 54 \qquad \text{we get} \qquad 54 = 133 - 1 \cdot 79.$$

Thus

$$\begin{aligned} 1 &= 13 \cdot 79 - 19 \cdot 54 \\ &= 13 \cdot 79 - 19 \cdot (133 - 1 \cdot 79) \\ &= 32 \cdot 79 - 19 \cdot 133. \end{aligned}$$

From

$$345 = 2 \cdot 133 + 79 \qquad \text{we get} \qquad 79 = 345 - 2 \cdot 133.$$

Thus

$$\begin{aligned} 1 &= 32 \cdot 79 - 19 \cdot 133 \\ &= 32 \cdot (345 - 2 \cdot 133) - 19 \cdot 133 \\ &= 32 \cdot 345 - 83 \cdot 133. \end{aligned}$$

Multiplying by 35 we get

$$35 = 32 \cdot 12075 - 83 \cdot 4655.$$

2.1.2 Suppose that m is a natural number that divides both $a + b$ and $a - b$. Then m divides $(a + b) + (a - b) = 2a$ and m divides $(a+b)-(a-b) = 2b$. Thus m is certainly not an odd prime. It follows that the greatest common divisor of $a - b$ and $a + b$ is a power of 2.

But $m = 4$ does not divide $2a$ and $2b$ so the greatest common divisor is either 1 or 2.
If $a + b$ is even then either a and b are both even or both odd. As a and b are coprime they are not both even. If a and b are odd then both $a + b$ and $a - b$ are even. Thus the greatest common divisor of $a + b$ and $a - b$ is either 1 or 2 and it is 2 if and only if both a and b are odd.
2.1.4 We may find common prime factorisations

$$a = p_1^{e_1} p_2^{e_2} \dots p_l^{e_l} \qquad b = p_1^{f_1} p_2^{f_2} \dots p_l^{f_l} \qquad \text{and} \qquad c = p_1^{g_1} p_2^{g_2} \dots p_l^{g_l}.$$

As b and c are coprime, it follows that if $f_i g_i = 0$ for all i. As $b|a$ it follows that $f_i \leq e_i$. As $c|a$ it follows that $g_i \leq e_i$. But then $f_i + g + i \leq e_i$, since one of f_i and g_i is zero. Thus

$$bc = p_1^{f_1+g_1} p_2^{f_2+g_2} \dots p_l^{f_l+g_l}$$

divides a.