MODEL ANSWERS TO THE THIRD HOMEWORK

2.2.1. It is convenient to use polar coordinates. Every complex number $\alpha = x + iy$ has an expression of the form

$$\alpha = re^{i\theta}$$

where r is the distance to the origin and θ is the angle the line, connecting the origin to (x, y), makes with the x-axis. In this case

$$s(\alpha) = r^2.$$

Suppose that we are given two Gaussian integers

$$\alpha = a + ib = re^{i\theta} \qquad \text{and} \qquad \beta = c + id = se^{i\phi}.$$

Then

$$\begin{aligned} \alpha\beta &= (re^{i\theta})(se^{i\phi}) \\ &= (rs)e^{i(\theta+\phi)}. \end{aligned}$$

Thus

$$\begin{aligned} s(\alpha\beta) &= r^2 s^2 \\ &= s(\alpha)s^2 \\ &\geq s(\alpha), \end{aligned}$$

with equality if and only if $s(\beta) = 1$. But $s(\beta) = 1$ implies $c^2 + d^2 = 1$ so that $c = \pm 1$ and $d = 0$ or $c = 0$ and $d = \pm 1$. In this case

$$\beta = \pm 1 \qquad \text{or} \qquad \beta = \pm i,$$

is a unit.

2.2.3. We may suppose that $m > 0$. Suppose that $m = ab$ where both $a > 1$ and $b > 1$ and $a \leq b$. Then

$$\begin{aligned} m &= ab \\ &> a^2, \end{aligned}$$

so that $a \leq \sqrt{m}$. Thus if m is not prime it has a divisor $1 < d \leq \sqrt{m}$. The Gaussian integers α such that $s(\alpha) = 1$ are precisely the units. If $\alpha = a + bi$ is a Gaussian integer then $s(\alpha) = a^2 + b^2$. Thus the possible values of $1 < s(\alpha) \leq 9$ are $2 = 1^2 + 1^2$, $4 = 2^2 + 0^2$, $5 = 2^2 + 1^2$, $8 = 2^2 + 2^2$ and $9 = 3^2 + 0^2$. On the other hand, if α is a non-zero Gaussian integer, then we can always find a unit u such that $u\alpha = c + di$ lies in the first quadrant, so that $c > 0$ and $d \geq 0$.

If $s(\alpha) = 2$ then $a = \pm 1$ and $b = \pm 1$. Multiplying by a unit our first prime is $p_1 = 1 + i$. $(1 + i)(1 - i) = 2$, so 2 is not prime and neither is $2 + 2i = 2(1 + i)$.
If $s(\alpha) = 4$ then $a = \pm 2$ and $b = 0$ or vice-versa. We have already seen that 2 is not a prime. If $s(\alpha) = 5$ then $a = \pm 2$ and $b = \pm 1$ or vice-versa. This gives us eight possibilities. Of those eight possibilities, two lie in the first quadrant, $2 + i$ and $1 + 2i$. These are the second $p_2 = 2 + i$ and third $p_3 = 1 + 2i$ primes up to units. The product of p_1 with p_2 or p_3 has norm squared bigger than nine. If $s(\alpha) = 8$ then $a = \pm 2$ and $b = \pm 2$. We have already seen that this is not prime. Finally suppose that $s(\alpha) = 9$ then $a = \pm 3$ and $b = 0$ or vice-versa. This gives one new prime, up to units, $p_4 = 3$.
Thus there are four primes α, 2, $2 + i$, $1 + 2i$ and 3, up to units, such that $s(\alpha) \leq 9$.
2.2.5. (a) Suppose that $f(x) \in \mathbb{Z}[x]$ divides both 2 and x. As $f(x)$ divides 2 it must be a constant. Thus $f(x) = a \in \mathbb{Z}$ is an integer. As this integer divides 2, $f(x) = \pm 1$ or $f(x) = \pm 2$. It is easy to see that ± 2 does not divide x. Thus the only common divisors of 2 and x are ± 1 and so the greatest common divisor is 1.
(b) If $\mathbb{Z}[x]$ were a Euclidean domain then we could find polynomials $p(x)$ and $q(x) \in \mathbb{Z}[x]$ such that

$$1 = 2p(x) + xq(x).$$

As the constant term of $xq(x)$ is zero and the constant term of $2p(x)$ is even, it follows that the constant term of the RHS is even, a contradiction.
2.2.9. Let

$$p(n) = 1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \cdots + \frac{1}{n}.$$

Let k be the largest integer such that $2^k \leq n$. Note that no other natural number between 1 and n is divisible by 2^k. Thus if we multiply both sides by 2^{k-1} every term

$$\frac{2^{k-1}}{i} \qquad \text{for} \qquad 1 \leq i \leq n, \qquad i \neq 2^k,$$

of the sum is odd.
As the sum of rational numbers with an odd denominator, has an odd denominator, it follows that $2^{k-1}p(n)$ is a sum of $1/2$ and a rational number an with odd denominator. In particular $p(n)$ is not an integer.
2.3.1. We find the greatest common divisor of 2072 and 1813. First we divide 1813 into 2072. We have

$$2072 = 1 \cdot 1813 + 259,$$

so that the quotient is 1 and the remainder is 259. Now we divide 259 into 1813. We have

$$1813 = 7 \cdot 259.$$

so that the quotient is 7 and the remainder is 0. Thus the greatest common divisor is 259.
Note that

$$2589 = 11 \cdot 259,$$

so that we can solve these equations.
Note that

$$2072 - 1813 = 259.$$

Multiplying through by 7 gives a solution to the equation

$$2072x + 1813y = 2849$$

Thus the general solution is

$$x = 1813k + 7 \qquad \text{and} \qquad y = -(2072k + 7).$$

2.3.3 Note that

$$1 = 1 \cdot 20 - 1 \cdot 19.$$

Thus

$$1909 = 1909 \cdot 20 - 1909 \cdot 19.$$

We are free to subtract $19k \cdot 20$ from the first sum and add $20k \cdot 19$ from the second sum. Thus the general solution to the equation

$$19x + 20y = 1909 \qquad \text{is} \qquad x = -1909 + 20k, y = 1909 - 19k.$$

If we want the first term to be positive we want

$$20k > 1909,$$

so that $k \geq 96$. If we want the second term to be positive we want

$$19k < 1909,$$

so that $k \leq 100$. The five solutions that lie in the interior of the first quadrant are

$$(x, y) = (11, 85) \quad (31, 66) \quad (51, 47) \quad (71, 28) \quad (91, 9).$$

2.3.7 We already know that the sum

$$by + cz$$

takes on any multiple of (b, c). Thus

$$by + cz = (b, c)\alpha,$$

for some integer α. It follows that a solution of the equation

$$ax + by + cz = d$$

is the same as a solution of the pair of equations

$$\begin{aligned} ax + (b,c)u &= d \\ by + cz &= (b,c). \end{aligned}$$

The general solution to the second equation is

$$y = y_0 + \frac{c}{(b,c)}s \qquad \text{and}$$

where $s \in \mathbb{Z}$ is any integer. Observe that

$$(a,b,c) = (a,(b,c)).$$

Therefore the general solution to the first equation is

$$x = x_0 + \frac{(b,c)}{(a,b,c)}t \qquad \text{and} \qquad u = u_0 - \frac{a}{(a,b,c)}t.$$

Thus the general solution to the equation

$$ax + by + cz = d$$

is

$$\begin{aligned} x &= x_0 + \frac{(b,c)}{(a,b,c)}t \\ y &= y_0 u_0 - \frac{ay_0}{(a,b,c)}t + \frac{c}{(b,c)}s \\ z &= z_0 - \frac{az_0}{(a,b,c)}t - \frac{b}{(b,c)}s. \end{aligned}$$

2.4.1 We first find the greatest common divisor. We have

$$\begin{aligned} 231896 &= 1 \cdot 198061 + 33835 \\ 198061 &= 5 \cdot 33835 + 28886 \\ 33835 &= 1 \cdot 28886 + 4949 \\ 28886 &= 5 \cdot 4949 + 4141 \\ 4949 &= 1 \cdot 4141 + 808 \\ 4141 &= 5 \cdot 808 + 101 \\ 808 &= 8 \cdot 101. \end{aligned}$$

Thus the greatest common divisor is 101. It follows that

$$\begin{aligned} [198061, 231896] &= \frac{198061 * 231896}{101} \\ &= 454748056. \end{aligned}$$

2.4.2 Suppose that $(a,b) = d$ and $[a,b] = m$. As $d|a$ and $a|m$ it follows that $d|m$.

Now suppose that $d|m$. Let $a = d$ and $b = m$. Then $d|a$ and $d|m$ and so it clear that $(a, b) = d$. Similarly $a|m$ and $b|m$ and so it is clear that $[a, b] = m$.

2.4.3. (a) We may assume that $y \geq z$. In this case

$$\max(y, z) = y.$$

Thus the LHS is

$$\min(x, y).$$

There are two cases. If $x \leq y$ then the LHS is x.
In this case

$$\min(x, y) = x \qquad \text{and} \qquad \min(x, z) = x.$$

Thus the RHS is also x.
Otherwise $x > y$. In this case the LHS is y and

$$\min(x, y) = y \qquad \text{and} \qquad \min(x, z) = z.$$

Thus the RHS is

$$\max(y, z) = y,$$

as well. Either way we have equality.
(b) We may find common prime factorisations

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

We can compute the LHS and the RHS prime by prime. The exponent of p_i on the LHS is

$$\min(e_i, \max(f_i, g_i))$$

and the exponent of p_i on the RHS is

$$\max(\min(e_i, f_i), \min(e_i, g_i)).$$

As these are equal, we have

$$(a, [b, c]) = ([a, b], [c, d]).$$

(c) Note first that

$$\begin{aligned}
\max(x, \min(y, z)) &= -\min(-x, \max(-y, -z)) \\
&= -\max(\min(-x, -y), \min(-x, -z)) \\
&= \min(\max(x, y), \min(x, z)).
\end{aligned}$$

We check that

$$[a, (b, c)] = ([a, b], [a.c]).$$

We pick common factorisations into primes, as in (b) and check this result prime by prime. The exponent of p_i on the LHS is

$$\max(e_i, \min(f_i, g_i))$$

and the exponent of p_i on the RHS is

$$\min(\max(e_i, f_i), \max(e_i, g_i)).$$

As these are equal, we have

$$[a, (b, c)] = ([a, b], [a.c]).$$

Let $a = b = 1$ and $c = 0$. Then

$$a + bc = 1 + 0 = 1 \qquad \text{and} \qquad (a + b)(a + c) = (1 + 1)(1 + 0) = 2 \neq 1.$$

Thus

$$a + bc \neq (a + b)(a + c).$$