1 Exercises

1.1

Which integers divide zero?

Using the definition, all $a \in \mathbb{Z}$ for which $\exists d \in \mathbb{Z}$ that satisfies $ad = 0$ divide 0. This condition holds for any a when $d = 0$, so all integers divide 0.

1.2

Show that if $a|b$ and $b|c$, then $a|c$.

$a|b \Rightarrow \exists m \in \mathbb{Z} \ni am = b$, $b|c \Rightarrow \exists n \in \mathbb{Z} \ni bn = c$. Rewriting, we have $amn = c$. $\therefore mn$ is an integer that divides c.

1.3

Prove that if $d|a$ then $d|ca$ for any integer c.

$a = dq \Rightarrow ca = cdq$, with $cq \in \mathbb{Z}$.

1.4

What are (4, 14), (5, 15) and (6, 16)?

2, 5, and 2.

1.5

What is (n, 1), where n is any positive integer? What is (n, 0)?

If $d = (n, 1)$, we have by (i) that $d|n$ and $d|1$. But, the only d that satisfies $d|1$ is 1, so $d = 1$.
If $d = (n, 0)$, we have by (i) that $d|n$ and $d|0$. We know from the first exercise that all $d \in \mathbb{Z}$ divide 0, so this is not helpful. So, it must be the greatest possible d that divides n, which is n.

1.6

If d is a positive integer, what is (d, nd)?

d divides nd, since $\exists q \ni qd = nd$, namely $q = n$. It also obviously divides d, since $1d = d$ (i). We cannot have a $c \in \mathbb{Z} \ni c > d$ for which the first condition holds, namely that $c|d$ (for nonzero d, $\nexists b \in \mathbb{Z} \ni bc = d$, only non-integer $b \in (0, 1)$) (ii).

1.7

What are q and r if $a = 75$ and $b = 24$? If $a = 75$ and $b = 25$?

$75 = 3 * 24 + 3$ ($q = 3$, $r = 3$). $75 = 3 * 25 + 0$ ($q = 3$, $r = 0$).

1.8

Verify that $a = bq + r \Rightarrow (a, b) = (b, r)$ when $a = 16$, $b = 6$, and $q = 2$.

$(a, b) = 2$, $(b, r) = 2$.

1.9

Calculate (343, 280) and (578, 442).

$$\begin{align} 343 &= 1 * 280 + 63 \tag{1}\\ 280 &= 4 * 63 + 28 \tag{2}\\ 63 &= 2 * 28 + 7 \tag{3}\\ 28 &= 4 * 7 + 0 \tag{4}\\ (343, 280) &= 7 \tag{5} \end{align}$$

$$\begin{align} 578 &= 1 * 442 + 136 \tag{6}\\ 442 &= 3 * 136 + 34 \tag{7}\\ 136 &= 4 * 34 + 0 \tag{8}\\ (578, 442) &= 34 \tag{9} \end{align}$$

2 Problems

2.1

Calculate (314, 159) and (4144, 7696).

$$\begin{align} 314 &= 1 * 159 + 155 \tag{10}\\ 159 &= 1 * 155 + 4 \tag{11}\\ 155 &= 38 * 4 + 3 \tag{12}\\ 4 &= 1 * 3 + 1 \tag{13}\\ 3 &= 3 * 1 + 0 \tag{14}\\ (314, 159) &= 1 \tag{15} \end{align}$$

$$\begin{align} 7696 &= 1 * 4144 + 3552 \tag{16}\\ 4144 &= 1 * 3552 + 592 \tag{17}\\ 3552 &= 6 * 592 + 0 \tag{18}\\ (4414, 7696) &= 592 \tag{19} \end{align}$$

2.2

Calculate (3141, 1592) and (10001, 100083).

$$\begin{align} 3141 &= 1 * 1592 + 1549 \tag{20}\\ 1592 &= 1 * 1549 + 43 \tag{21}\\ 1549 &= 36 * 43 + 1 \tag{22}\\ 43 &= 43 * 1 + 0 \tag{23}\\ (3141, 1592) &= 1 \tag{24} \end{align}$$

$$\begin{align} 100083 &= 10 * 10001 + 73 \tag{25}\\ 10001 &= 137 * 73 + 0 \tag{26}\\ (10001, 100083) &= 73 \tag{27} \end{align}$$

2.3

Find x and y such that 314x + 159y = 1.

$$1 = 4 - 1 * 3 \tag{28}$$
$$1 = 4 - 1 * (155 - 38 * 4) \tag{29}$$
$$1 = 39 * 4 - 155 \tag{30}$$
$$1 = 39 * (159 - 155) - 155 \tag{31}$$
$$1 = 39 * 159 - 40 * 155 \tag{32}$$
$$1 = 39 * 159 - 40 * (314 - 159) \tag{33}$$
$$1 = 314 * (-40) + 159 * 79 \tag{34}$$

2.4

Find x and y such that 4144x + 7696y = 592.

$$592 = 4144 - 1 * 3552 \tag{35}$$
$$592 = 4144 - 1 * (7696 - 4144) \tag{36}$$
$$592 = 4144 * 2 - 7696 * 1 \tag{37}$$

2.5

If $N = abc + 1$, prove that $(N, a) = (N, b) = (N, c) = 1$.

1 is certainly a divisor of N, a, b, and c, so the only thing left to show is that 1 is the greatest divisor of each. Assume $\exists k \ni k > 1, k|N$ and $k|a$. Plug in the definition of N to get $k|abc + 1$. Then $\exists y \ni ky = a$, $\exists x \ni kx = abc + 1$. Combine the two to get $kx = kybc + 1 \Rightarrow k(x - ybc) = 1$. For $k, x, y, b, c \in \mathbb{Z}$, only $k = 1, x - ybc = 1$ or $k = -1, x - ybc = -1$ fulfill the equation. Since both $k = -1$ and $k = 1$ contradict the assumption that $k > 1$, 1 must be the greatest divisor of (N, a). One could analogously show this property for b and c.

2.6

Find two different solutions of 299x + 247y = 13.

$$299 = 1 * 247 + 52 \tag{38}$$
$$247 = 4 * 52 + 39 \tag{39}$$
$$52 = 1 * 39 + 13 \tag{40}$$

$$13 = 52 - 39 \tag{41}$$
$$13 = 52 - (247 - 4 * 52) \tag{42}$$
$$13 = 5 * 52 - 247 \tag{43}$$
$$13 = 5 * (299 - 247) - 247 \tag{44}$$
$$13 = 5 * 299 - 6 * 247 \tag{45}$$

Observe that $13 = 52 - 39 = 4 * 13 - 3 * 13$. Pick $a, b \ni 3a - 4b = 1$, or $a = \frac{1+4b}{3}$, for example $a = 3$, $b = 2$. Then

$$13 = 3 * 3 * 13 - 2 * 4 * 13 \tag{46}$$
$$13 = 3 * 39 - 2 * 52 \tag{47}$$
$$13 = 3 * (247 - 4 * 52) - 2 * 52 \tag{48}$$
$$13 = 3 * 247 - 14 * 52 \tag{49}$$
$$13 = 3 * 247 - 14 * (299 - 247) \tag{50}$$
$$13 = 17 * 247 - 14 * 299 \tag{51}$$
$$\tag{52}$$

2.7

Prove that if $a|b$ and $b|a$ then $a = b$ or $a = -b$.

If $a|b$ then $\exists x \in \mathbb{Z} \ni ax = b$. If $b|a$ then $\exists y \in \mathbb{Z} \ni by = a$. Combining, have $bxy = b \Rightarrow xy = 1$. The only two solutions to this equation in the domain of integers are $(1, 1)$ and $(-1, -1)$. So, $ax = b \Rightarrow a = b$ when $x = 1$, $a = -b$ when $x = -1$.

2.8

Prove that if $a|b$ and $a > 0$, then $(a, b) = a$.

a is a divisor of a since $1a = a$, and b since it is given. It remains to show that a is the greatest common divisor of a and b. Assume $\exists c \ni c > a > 0, c|a, c|b$. Then $\exists x \ni cx = a$. Since c and a are both greater than 0, we need $x > 0$ for the equality to hold. But even at $x = 1$, the smallest $x \in \mathbb{Z} \ni x > 0$, $c > a$. So there are no such x or c.

2.9

Prove that $((a, b), b) = (a, b)$.

By the definition of $(x, y) = d$, $d|x$ and $d|y$. So, $(a, b)|b$. Now we must show that (a, b) is the greatest common divisor of (a, b) and b. Assume $\exists c \ni c > (a, b), c|(a, b), c|b$. Similarly to exercise 8, if $(a, b) > 0$, can't have an $x \in \mathbb{Z}^+ \ni cx = (a, b)$.
Let $(a, b) = d \ni d < 0$. So $\exists y, z \in \mathbb{Z} \ni y * d = a, z * d = b$. But then $-y * -d = a$, $-z * -d = b$, so d is a divisor of both a and b and $-d > d$ and $(a, b) \neq d$.

2.10

(a) Prove that $(n, n + 1) = 1$ for all $n > 0$.
(b) If $n > 0$, what can $(n, n + 2)$ be?

(a) $1|n$ and $1|n + 1$ since $\forall x \in \mathbb{Z}, 1x = x$. Suppose $\exists k > 1 \ni k|n, k|n + 1$. So $\exists x \ni kx = n$ and $\exists y \ni ky = n + 1$. Combine the two to get $ky = kx + 1 \Rightarrow k(y - x) = 1$. The only viable pairs of $k, (y - x) \in \mathbb{Z}$ for which the equality holds are $(1, 1)$ and $(-1, -1)$, both of which violate the assumption that $k > 1$.
(b) Similarly to above, $\exists k \ni k|n, k|n+2 \Rightarrow \exists x, y \ni kx = n, ky = n+2$. So $ky = kx+2 \Rightarrow k(y-x) = 2$. Since GCDs must be positive, as shown in the previous exercise, we can have $k = 1$ when $(y - x) = 2$ or $k = 2$ when $(y - x) = 1$.

2.11

(a) Prove that $(k, n + k) = 1$ iff $(k, n) = 1$.
(b) Is it true that $(k, n + k) = d$ iff $(k, n) = d$?

(a) First, we show $(k, n) = 1 \Rightarrow (k, n + k) = 1$. Let $(k, n + k) = d \ni d > 1$. By the definition of the GCD, we know $d|k, d|n + k$. So $\exists a, b \ni ad = k, bd = n + k$. This means $d(b - a) = n$, implying $d|n$. From the given $(k, n) = 1$, we know that any $\forall c, c|k, c|n \Rightarrow c \leq 1$, so we have a contradiction.
Next, we show $(k, n + k) = 1 \Rightarrow (k, n) = 1$. By **Lemma 1**, $\forall c \ni c|k, c|n + k \Rightarrow c|k + n + k$ and $(k, n + k) = 1 \Rightarrow c \leq 1$. Let $(k, n) = d \ni d > 1$. By the GCD defintion, $d|k$, and by an application of **Lemma 1**, $d|n + k$. Applying **Lemma 1** again, $d|k, d|n + k \Rightarrow d|k + n + k$. But, we've shown that such $d \leq 1$, so we have a contradiction.
(b) First, show $(k, n) = d \Rightarrow (k, n + k) = d$. Assume $\exists q \ni q|k, q|n + k, q > d$. Like in **(a)**, we know that $q|k, q|n + k \Rightarrow q|n$. This contradicts $(k, n) = d$.
Now show $(k, n+k) = d \Rightarrow (k, n) = d$. Like in **(a)**, we know that $d|k, d|n+k \Rightarrow d|n$. So d is definitely a divisor for n and k. Assume $\exists c \ni c|n, c|k, c > d$. $c|n, c|k \Rightarrow c|n + k$, which would contradict $(k, n + k) = d$.
So yes, the statement holds.

2.12

Prove: If $a|b$ and $c|d$, then $ac|bd$.

$\exists x, y \ni ax = b, cy = d$. So $bd = (ac)(xy)$ and $ac|bd$.

2.13

Prove: If $d|a$ and $d|b$, then $d^2|ab$.

$\exists x, y \ni dx = a, dy = b$. So $ab = d^2xy$ and $d^2|ab$.

2.14

Prove: If $c|ab$ and $(c, a) = d$, then $c|db$.

Since $(c, a) = d$, we can write $a = dx, c = dy \ni x, y \leq d$. Furthermore, $(x, y) = 1$ because if there were a $z > 1 \ni z|x, z|y$, then $dz|a$ and $dz|c$ with $dz > d$, violating the GCD definition. We rewrite $ab = dxb \ni c|dxb$. Subbing in the new definition for c, $dy|dxb$, i.e. $y|xb$. By **Corollary 1**, if $y|xb$ and $(x, y) = 1$, then $y|b$. So $dy|db$, i.e. $c|db$.

2.15

(a) If $x^2 + ax + b = 0$ has an integer root, show that it divides b.
(b) If $x^2 + ax + b = 0$ has a rational root, show that it is in fact an integer.

(a) Assuming a and b are integers. $b = -x^2 - ax = x(-x - a)$. Since a, x are both integers, their linear combinations are integers as well. So $\exists q \in \mathbb{Z} \ni bq = x$, namely $q = -x - a$.
(b) If x is rational, it can be written as $\frac{n}{k} \ni n \in \mathbb{Z}, k \in \mathbb{Z}^+$ and n, k are relatively prime. Subbing in, have $(\frac{n}{k})^2 + a\frac{n}{k} + b = 0$. Can rewrite this as $-k(bk + an) = n^2$. This implies $k|n^2$. Since n, k are relatively prime, $(n, k) = 1$. Using the result from exercise **14**, $k|nn$ and $(n, k) = 1 \Rightarrow k|1n$. If $k|n$ and $k|k$ and $(n, k) = 1$, then $k = 1$ and $\frac{n}{k} = n$, with $n \in \mathbb{Z}$.