SOLUTIONS TO PROBLEM SET 1

SECTION 1.3

Exercise 4. We see that
\[
\frac{1}{1 \cdot 2} = \frac{1}{2}, \quad \frac{1}{1 \cdot 2} + \frac{1}{2 \cdot 3} = \frac{2}{3}, \quad \frac{1}{1 \cdot 2} + \frac{1}{2 \cdot 3} + \frac{1}{3 \cdot 4} = \frac{3}{4},
\]
and is reasonable to conjecture
\[
\sum_{k=1}^{n} \frac{1}{k(k+1)} = \frac{n}{n+1}.
\]
We will prove this formula by induction.

Base \( n = 1 \): It is shown above.

Hypothesis: Suppose the formula holds for \( n \).

Step:
\[
\sum_{k=1}^{n+1} \frac{1}{k(k+1)} = \sum_{k=1}^{n} \frac{1}{k(k+1)} + \frac{1}{(n+1)(n+2)}
= \frac{n}{n+1} + \frac{1}{(n+1)(n+2)}
= \frac{n(n+2)+1}{(n+1)(n+2)}
= \frac{n^2 + 2n + 1}{(n+1)(n+2)}
= \frac{(n+1)^2}{(n+1)(n+2)} = \frac{n+1}{n+2},
\]
where in the second equality we used the induction hypothesis.

Exercise 14. We will use strong induction.

Base \( 54 \leq n \leq 60 \): We have
\[
54 = 7 \cdot 2 + 10 \cdot 4, \quad 55 = 7 \cdot 5 + 10 \cdot 2, \quad 56 = 7 \cdot 8 + 10 \cdot 0, \quad 57 = 7 \cdot 1 + 10 \cdot 5
\]
and
\[
58 = 7 \cdot 4 + 10 \cdot 3, \quad 59 = 7 \cdot 7 + 10 \cdot 1, \quad 60 = 7 \cdot 0 + 10 \cdot 6.
\]

Hypothesis: Suppose the result holds for \( 54 \leq k \leq n \).

Step \( n \geq 60 \): We have \( n - 6 \geq 54 \), hence by the induction hypothesis we can write
\[
n - 6 = 7a + 10b \quad \text{for some } a, b \in \mathbb{Z}_{>0}.
\]
Then \( n + 1 = 7(a + 1) + 10b \), as desired.
Exercise 22. We will use induction.

Base $n = 0$: We have $1 + 0h = 1 = (1 + h)^0$, as desired.

Hypothesis: Suppose the result holds for $n$.

Step $n \geq 0$: We have

$$(1 + h)^{n+1} = (1 + h)^n (1 + h)$$
$$\geq (1 + nh)(1 + h)$$
$$= 1 + nh + nh^2$$
$$\geq 1 + (n + 1)h,$$

where in the first inequality we used the induction hypothesis and $1 + h \geq 0$.

Exercise 24. The proof fails in the statement that the sets $\{1, \ldots, n\}$ and $\{2, \ldots, n + 1\}$ have common members. This is false when $n = 1$; indeed, the sets are $\{1\}$ and $\{2\}$ which are clearly disjoint.

Section 1.5

Exercise 26. Let $a, b \in \mathbb{Z}_{>0}$.

We first prove existence. The division algorithm gives $q', r' \in \mathbb{Z}$ such that

$$a = bq' + r' \quad \text{with} \quad 0 \leq r' < b.$$

We now divide into two cases:

(i) Suppose $r' \leq b/2$; then $-b/2 < r' \leq b/2$. The result follows by taking $q = q'$ and $r = r'$.

(ii) Suppose $b/2 < r' < b$; then $-b/2 < r' - b < 0$. We have

$$a = bq' + r' = bq' + b + r' - b = b(q' + 1) + (r' - b),$$

Write $q = q' + 1$ and $r = r' - b$. Then

$$a = bq + r, \quad \text{with} \quad -b/2 < r < 0 \leq b/2.$$

as desired.

We now prove uniqueness. Suppose

$$a = bq_1 + r_1 = bq_2 + r_2, \quad \text{with} \quad -b/2 < r_1, r_2 \leq b/2.$$ 

Then $b(q_1 - q_2) = (r_2 - r_1)$ and $b$ divides $r_2 - r_1$. Since $-b < r_2 - r_1 < b$ it follows that $r_2 - r_1 = 0$ because there is no other multiple of $b$ in this interval. We conclude that $r_1 = r_2$ and $b(q_1 - q_2) = 0$; thus we also have $q_1 = q_2$, as desired.

Exercise 36. Let $a \in \mathbb{Z}$. Dividing $a$ by 3 we get $a = 3q + r$ with $r = 0, 1, 2$. Note that

$$a^3 - a = (a - 1)a(a + 1) = (3q + r - 1)(3q + r)(3q + r + 1)$$

and clearly for any choice of $r = 0, 1, 2$ one of the three factors is a multiple of 3. This is the same as saying that in among three consecutive integers one must be a multiple of 3.
Exercise 12. Let $a \in \mathbb{Z}_{>0}$.

We first prove existence. We will use strong induction.

**Base $a \leq 2$.** If $a = 1$ take $k = 0$ and $e_0 = 1$; if $a = 2$ take $k = 1$, $e_1 = 1$ and $e_0 = -1$.

**Hypothesis:** Suppose the desired expression exists for all positive integers $< a$.

**Step $a \geq 3$.** From the modified division algorithm (Problem 26 in Section 1.5) there exist $q, e_0 \in \mathbb{Z}$ such that

$$a = 3q + r, \quad \text{with} \quad -3/2 < r \leq 3/2;$$

in particular, $r = -1, 0, 1$. We have $0 < q = (a - r)/3 < a$ and by hypothesis we can write

$$q = a_s 3^s + \ldots + a_1 3 + a_0, \quad a_s \neq 0, \quad a_i \in \{-1, 0, 1\}.$$

Thus we have

$$a = 3q + r = 3(a_s 3^s + \ldots + a_1 3 + a_0) + r = a_s 3^{s+1} + \ldots + a_1 3^2 + a_0 3 + r$$

and we take $k = s + 1$, $e_0 = r$ and $e_i = a_{s-i}$ for $i = 1, \ldots, k$.

We now prove uniqueness. We will use strong induction. Suppose

$$a = e_k 3^k + \ldots + e_1 3 + e_0 = c_s 3^s + \ldots + c_1 3 + c_0, \quad e_k, a_s \neq 0, \quad e_i, a_i \in \{-1, 0, 1\}.$$

**Base $a \leq 2$:** We know from above that if $a = 1$ can we take $k = 0$ and $e_0 = 1$ and if $a = 2$ we can take $k = 1$, $e_1 = 1$ and $e_0 = -1$, as balanced ternary expansions. Note also that 0 cannot be written as an expansion using non-zero coefficients.

Suppose now $a = 1 = e_k 3^k + \ldots + e_1 3 + e_0$ with $k \geq 1$; then $a$ divided by 3 has reminder $e_0 = 1$ by the division algorithm. We conclude that $e_k 3^k + \ldots + e_1 3 = 0$ which is impossible, unless $e_i = 0$ for all $i \geq 1$.

Suppose $a = 2 = 1 \cdot 3 - 1 = e_k 3^k + \ldots + e_1 3 + e_0$ with $k \geq 1$; then $a$ divided by 3 has reminder $e_0 = -1$ by the modified division algorithm. We conclude that $e_k 3^k + \ldots + e_1 3 = 3$. Dividing both sides by 3 we conclude that $e_k 3^{k-1} + \ldots + e_1 = 1$ which gives $k = 1$ and $e_1 = 1$ by the previous paragraph. This shows that $a = 1, 2$ have an unique balanced ternary expansion.

**Hypothesis:** Suppose the expansion is unique for all positive integers $< a$.

**Step $a \geq 3$:** By the uniqueness of the modified division algorithm (Problem 26, Section 1.5), dividing $a$ by 3 we conclude $e_0 = c_0$. Now

$$\frac{a - e_0}{3} = e_k 3^{k-1} + \ldots + e_1 = c_s 3^{s-1} + \ldots + c_1$$

and by induction hypothesis we have $k = s$ and $e_i = c_i$ for $i = 1, \ldots, k$.

Finally, suppose $a < 0$; we apply the result to $-a > 0$ and (due to the symmetry of the coefficients) we obtain the expansion for $a$ by multiplying by $-1$ the expansion for $-a$.

Exercise 13. Let $w$ be the weight to be measured. From the previous exercise we can write

$$w = e_k 3^k + \ldots + e_1 3 + e_0, \quad e_k \neq 0, \quad e_i \in \{-1, 0, 1\}.$$

Place the object in pan 1. If $e_i = 1$, then place a weight of $3^i$ into pan 2; if $e_i = -1$, then place a weight of $3^i$ into pan 1; if $e_i = 0$ do nothing; in the end the pans are balanced.
Exercise 17. Let \( n \in \mathbb{Z}_{\geq 0} \) be given in base \( b \) by
\[
n = a_k b^k + \ldots + a_1 b + a_0, \quad a_k \neq 0, \quad 0 \leq a_i < b.
\]
Let \( m \in \mathbb{Z}_{>0} \). We want to find the base \( b \) expansion of \( b^m n \), that is
\[
b^m n = c_s b^s + \ldots + c_1 b + c_0, \quad c_s \neq 0, \quad 0 \leq c_i < b.
\]
Multiplying both sides of the first equation by \( b^m \) gives
\[
b^m n = a_k b^{k+m} + \ldots + a_1 b^{m+1} + a_0 b^m, \quad a_k \neq 0, \quad 0 \leq a_i < b.
\]
We know that the expansion in base \( b \) is unique, so by comparing the last two equations we conclude that
\[
s = k + m, \quad c_{s-i} = a_{k-i} \text{ for } i = 0, \ldots, k \quad \text{and} \quad c_i = 0 \text{ for } i = 0, \ldots, m-1,
\]
which means
\[
b^m n = (c_s c_{s-1} \ldots c_0)_b = (a_k a_{k-1} \ldots a_1 a_0 00 \ldots 0)_b,
\]
where we have \( m \) zeros in the end.

Section 3.1

Exercise 6. Let \( n \in \mathbb{Z} \). Note the factorization \( n^3 + 1 = (n+1)(n^2 - n + 1) \) into two integers. If \( n^3 + 1 \) is a prime, then \( n \geq 1 \) and \( n + 1 \) is either 1 or prime. Since \( n + 1 \neq 1 \) we have \( n + 1 \) is prime and hence \( n^2 - n + 1 \) must be 1, which implies \( n = 0, 1 \). We conclude \( n = 1 \), as desired.

Exercise 8. Let \( n \geq \mathbb{Z}_{\geq 0} \). Consider \( Q_n = n! + 1 \). There is a prime factor \( p \mid Q_n \). Suppose \( p \leq n \); then \( p \mid n! = n(n-1)(n-2)\ldots 2 \cdot 1 \) therefore \( p \mid Q_n - n! = 1 \), a contradiction. We conclude that \( p > n \). In particular, given a positive integer \( n \) we can always find a prime larger than \( n \); by growing \( n \) we produce infinitely many arbitrarily large primes.

Exercise 9. Note that if \( n \leq 2 \), then \( S_n \leq 1 \). Therefore, we must assume that \( n \geq 3 \) so that \( S_n > 1 \). It follows then that \( S_n \) has a prime divisor \( p \). If \( p \leq n \), then \( p \mid n! \), and so \( p \mid (n! - S_n) = 1 \), a contradiction. Thus \( p > n \). Because we can find arbitrarily large primes, there must be infinitely many.

Section 3.3

Exercise 6. Let \( a \in \mathbb{Z}_{>0} \) and write \( d = (a, a + 2) \). In particular, \( d \) divides both \( a \) and \( a + 2 \), hence \( d \) also divides the difference \( (a + 2) - a = 2 \). We conclude \( d = 1 \) or \( d = 2 \). Now, if \( a \) is odd then \( a + 2 \) is also odd, hence \( d = 1 \); if \( a \) is even then \( 2 \) divides both \( a \) and \( a + 2 \), so \( d = 2 \). We conclude that \( (a, a + 2) = 1 \) if and only if \( a \) is odd and \( (a, a + 2) = 2 \) if and only if \( a \) is even.

Exercise 10. Write \( d = (a + b, a - b) \). If \( d = 1 \) there is nothing to prove. Suppose \( d \neq 1 \) and let \( p \) be a prime divisor of \( d \) (which exists because \( d \neq 1 \)). In particular, \( p \) is a common divisor of \( a + b \) and \( a - b \), therefore it divides both their sum and difference; more precisely, \( p \) divides
\[
(a + b) + (a - b) = 2a \quad \text{and} \quad (a + b) - (a - b) = 2b.
\]
Furthermore, since \( p \) is prime we also have
\[
(i) \quad p \mid 2a \text{ implies } p = 2 \text{ or } p \mid a,
\]

4
(ii) \( p | 2b \) implies \( p = 2 \) or \( p | b \).

Suppose \( p \neq 2 \). Then in (i) we have \( p | a \) and in (ii) we have \( p | b \); this is a contradiction with \( (a, b) = 1 \). We conclude that \( p = 2 \).

So far we have shown that the unique prime factor of \( d \) is 2, therefore \( d = 2^k \) with \( k \geq 1 \). To finish the proof we need to prove that \( k = 1 \). Since \( d | a + b \) and \( d | a - b \) arguing as above we conclude that \( 2^k | 2a \) and \( 2^k | 2b \), that is

\[
2a = 2^k x \quad \text{and} \quad 2b = 2^k y \quad \text{for some} \ x, y \in \mathbb{Z}.
\]

Suppose \( k \geq 2 \). Then dividing both equations by 2 we get

\[
a = 2^{k-1} x \quad \text{and} \quad b = 2^{k-1} y
\]

with \( k - 1 \geq 1 \). In particular \( 2 | a \) and \( 2 | b \), a contradiction with \( (a, b) = 1 \), showing that \( k = 1 \), as desired.

**Here is an alternative, shorter proof using one of the main theorems on \( \gcd \):**

Let \( a, b \in \mathbb{Z} \) satisfy \( (a, b) = 1 \). There exist \( x, y \in \mathbb{Z} \) such that \( ax + by = 1 \). Then

\[
(a + b)(x + y) + (a - b)(x - y) = 2ax + 2by = 2(ax + by) = 2
\]

and since \( (a + b, a - b) \) is the smallest positive integer that can be written as an integral linear combination of \( a + b \) and \( a - b \) we must have \( (a + b, a - b) \leq 2 \). Thus \( (a + b, a - b) = 1, 2 \) as desired.

**Exercise 12.** Let \( a, b \in \mathbb{Z} \) be even and not both zero. There exist \( x, y \in \mathbb{Z} \) such that

\[
ax + by = (a, b) \iff \frac{a}{2}x + \frac{b}{2}y = \frac{(a, b)}{2}.
\]

Since \((a/2, b/2)\) is the smallest positive integer that can be written as an integral linear combination of \( a/2 \) and \( b/2 \) we must have \((a/2, b/2) \leq (a, b)/2\).

To finish the proof we will show that \((a/2, b/2) \geq (a, b)/2\). There exist \( x, y \in \mathbb{Z} \) such that

\[
\frac{a}{2}x + \frac{b}{2}y = (a/2, b/2) \iff ax + by = 2(a/2, b/2).
\]

Since \( (a, b) \) is the smallest positive integer that can be written as an integral linear combination of \( a \) and \( b \) we conclude \( (a/2, b/2) \geq (a, b)/2 \), as desired.

**Exercise 24.** Let \( k \in \mathbb{Z}_{>0} \). Suppose \( d \) is a common divisor of \( 3k + 2 \) and \( 5k + 3 \). Then \( d \) divides every integral linear combination of these numbers. In particular, \( d \) divides

\[
5(3k + 2) - 3(5k + 3) = 15k + 10 - 15k - 9 = 1,
\]

hence \((3k + 2, 5k + 3) = 1\), as desired.
Exercise 2. We will use the Euclidean algorithm.

a) Compute $(51, 87)$.
\[87 = 51 \cdot 1 + 36, \quad 51 = 36 \cdot 1 + 15, \quad 36 = 15 \cdot 2 + 6, \quad 15 = 6 \cdot 2 + 3, \quad 6 = 3 \cdot 2 + 0,\]
thus $(51, 87) = 3$.

b) Compute $(105, 300)$.
\[300 = 105 \cdot 2 + 90, \quad 105 = 90 \cdot 1 + 15, \quad 90 = 15 \cdot 6 + 0,\]
thus $(105, 300) = 15$.

c) Compute $(981, 1234)$.
\[1234 = 981 \cdot 1 + 253, \quad 981 = 253 \cdot 3 + 222, \quad 253 = 222 \cdot 1 + 31\]
and
\[222 = 31 \cdot 7 + 5, \quad 31 = 5 \cdot 6 + 1, \quad 5 = 1 \cdot 5 + 0,\]
thus $(981, 1234) = 1$.

Exercise 6.

a) Compute $(15, 35, 90)$.
Note that $90 = 15 \cdot 6$ then $((15, 90), 35) = (15, 35) = 5$.

b) Compute $(300, 2160, 5040)$.
Note that $1260 = 300 \cdot 7 + 60$ and $300 = 60 \cdot 5$ thus $(300, 2160) = 60$.
Since $5040 = 60 \cdot 84$ we also have
\[(300, 2160, 5040) = ((300, 2160), 5040) = (60, 5040) = 60.\]

Exercise 10. Let $a, b \in \mathbb{Z}_{>0}$. Suppose $a^3 \mid b^2$.

Write $a = p_1^{a_1} p_2^{a_2} \ldots p_k^{a_k}$ for the prime factorization of $a$. Write $p_i^{b_i}$ for the largest power of $p_i$ dividing $b$. In particular, we can write $b = p_i^{b_i} \cdot m$ for some $m \in \mathbb{Z}$, with $p_i \nmid m$.

From $a^3 \mid b^2$ it follows that $p_i^{3a_i} \mid p_i^{2b_i} m^2$ and since $p_i \nmid m$ we must have $p_i^{3a_i} \mid p_i^{2b_i}$. This implies $2b_i - 3a_i \geq 0$, hence $b_i/a_i \geq 3/2 > 1$. Thus $b_i > a_i$ for all $i$. Hence we can write
\[b = p_1^{a_1} p_1^{b_1-a_1} \cdot p_2^{a_2} p_2^{b_2-a_2} \cdot \ldots \cdot p_k^{a_k} p_k^{b_k-a_k} \cdot m'\]
for some $m' \in \mathbb{Z}$ (note that $m'$ is needed since $b$ may have prime factors which are none of the $p_i$). Therefore, by reordering the factors we also have
\[b = (p_1^{a_1} p_2^{a_2} \ldots p_k^{a_k})(p_1^{b_1-a_1} p_2^{b_2-a_2} \ldots p_k^{b_k-a_k}) \cdot m' = a(p_1^{b_1-a_1} p_2^{b_2-a_2} \ldots p_k^{b_k-a_k}) \cdot m'.\]
Thus $a \mid b$, as desired.
Exercise 30. We will use the formulas for \((a, b)\) and \(\text{LCM}(a, b)\) in terms of the prime factorizations of \(a\) and \(b\).

a) \(a = 2 \cdot 3^2 \cdot 5^3, b = 2^2 \cdot 3^3 \cdot 7^2\). Thus
\[
(a, b) = 2 \cdot 3^2, \quad \text{LCM}(a, b) = 2^2 \cdot 3^3 \cdot 5^3 \cdot 7^2.
\]

b) \(a = 2 \cdot 3 \cdot 5 \cdot 7, b = 7 \cdot 11 \cdot 13\). Thus
\[
(a, b) = 7, \quad \text{LCM}(a, b) = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13.
\]

c) \(a = 2^8 \cdot 3^6 \cdot 5^4 \cdot 11^{13}, b = 2 \cdot 3 \cdot 5 \cdot 11 \cdot 13\). Thus
\[
(a, b) = 2 \cdot 3 \cdot 5 \cdot 11, \quad \text{LCM}(a, b) = 2^8 \cdot 3^6 \cdot 5^4 \cdot 11^{13} \cdot 13.
\]

d) \(a = 41^{101} \cdot 47^{43} \cdot 103^{1001}, b = 41^{11} \cdot 43^{47} \cdot 83^{111}\). Thus
\[
(a, b) = 41^{11}, \quad \text{LCM}(a, b) = 41^{101} \cdot 43^{47} \cdot 47^{43} \cdot 83^{111} \cdot 103^{1001}.
\]

Exercise 34. Let \(a, b \in \mathbb{Z}_{\geq 0}\). Suppose that
\[
(a, b) = 18 = 2 \cdot 3^2 \quad \text{and} \quad \text{LCM}(a, b) = 540 = 2^3 \cdot 3^3 \cdot 5.
\]

Since \((a, b) \cdot \text{LCM}(a, b) = ab\) we conclude that the possible prime factors of \(a, b\) are 2, 3 and 5. Write
\[
a = 2^{d_2}3^{d_3}5^{d_5}, \quad b = 2^{e_2}3^{e_3}5^{e_5}, \quad d_i, e_i \geq 0
\]
for the prime factorizations of \(a\) and \(b\). We also know that
\[
(a, b) = 2^{\min(d_2, e_2)} \cdot 3^{\min(d_3, e_3)} \cdot 5^{\min(d_5, e_5)}
\]
and
\[
\text{LCM}(a, b) = 2^{\max(d_2, e_2)} \cdot 3^{\max(d_3, e_3)} \cdot 5^{\max(d_5, e_5)}.
\]

Therefore,
\[
\min(d_2, e_2) = 1 \quad \max(d_2, e_2) = 2.
\]

After interchanging \(a, b\) if necessary we can suppose \(d_2 = 1\) and \(e_2 = 2\). Similarly, we also have
\[
\min(d_3, e_3) = 2, \quad \max(d_3, e_3) = 3, \quad \min(d_5, e_5) = 0, \quad \max(d_5, e_5) = 1.
\]

Thus \((d_3, e_3) = (2, 3)\) or \((3, 2)\) and \((d_5, e_5) = (1, 0)\) or \((1, 0)\), giving the following four possibilities for \(a, b\):

1. \(a = 2^1 \cdot 3^2 = 18\) and \(b = 2^2 \cdot 3^3 \cdot 5^1 = 540\),
2. \(a = 2^1 \cdot 3^2 \cdot 5^1 = 90\) and \(b = 2^2 \cdot 3^3 = 108\),
3. \(a = 2^1 \cdot 3^3 = 54\) and \(b = 2^2 \cdot 3^2 \cdot 5^1 = 180\),
4. \(a = 2^1 \cdot 3^3 \cdot 5^1 = 270\) and \(b = 2^2 \cdot 3^2 = 36\),

Since \((a, b)\) and \(\text{LCM}(a, b)\) do not depend on the signs and order of \(a, b\) we obtain all the solutions by multiplying \(a\) or \(b\) or both by \(-1\) and interchanging them: \((\pm 18, \pm 540), (\pm 540, \pm 18), (\pm 90, \pm 108), (\pm 108, \pm 90), (\pm 54, \pm 180), (\pm 180, \pm 54), (\pm 270, \pm 36), (\pm 36, \pm 270)\).

The following argument, avoiding the formula \((a, b) \cdot \text{LCM}(a, b) = ab\), is an alternative to the first part of the proof above. Write
\[
a = 7^{e_1} \ldots p_k^{e_k}, \quad b = 7^{d_1} \ldots p_k^{d_k}, \quad e_i, d_i \geq 0
\]
(note that we have to allow the exponents to be zero so that we can use the same primes \( p_i \) in both factorizations). We have that

\[ 18 = 2 \cdot 3^2 = (a, b) = p_1^{\min(e_1,d_1)} \cdots p_k^{\min(e_k,d_k)}, \]

hence \( p_1 = 2, \min(e_1,d_1) = 1, p_2 = 3, \min(e_2,d_2) = 2 \) and \( \min(e_i,d_i) = 0 \) for all \( i \) satisfying \( 3 \leq i \leq k \). We also have,

\[ 540 = 2^2 \cdot 3^3 \cdot 5 = \text{LCM}(a, b) = p_1^{\max(e_1,d_1)} \cdots p_k^{\max(e_k,d_k)}, \]

hence \( \max(e_1,d_1) = 2, \max(e_2,d_2) = 3, p_3 = 5, \max(e_3,d_3) = 1 \) and \( \max(e_i,d_i) = 0 \) for all \( i \) satisfying \( 4 \leq i \leq k \). Thus \( e_i = d_i = 0 \) for all \( i \) satisfying \( 4 \leq i \leq k \). Note this argument gives at the same time that the prime factors of \( a \) and \( b \) are 2, 3 or 5 and information about the possible exponents they may occur.

**Exercise 42.**

\( a \) Suppose \( \sqrt[3]{5} \) is rational. Then, \( \sqrt[3]{5} = a/b \) for some coprime positive integers \( a, b \) with \( b \neq 0 \). Then, we have

\[ \sqrt[3]{5} = a/b \implies 5b^3 = a^3 \implies 5 \divides a \]

because 5 is a prime dividing the product \( a^3 = aaa \), so divides one of the factors. Therefore, \( a = 5k \) for some \( k \in \mathbb{Z} \) and, replacing above gives

\[ 5b^3 = (5k)^3 \iff b^3 = 5^2k^3 \implies 5 \divides b, \]

showing that both \( a, b \) are divisible by 5, a contradiction.

\( b \) Let \( f(x) = x^3 - 5 \), which is a monic polynomial with integer coefficients. We have \( f(\sqrt[3]{5}) = 0 \) and since \( \sqrt[3]{5} \) is not an integer it must be irrational by Theorem 3.18 (in the textbook).

**Exercise 45.** Suppose that \( \log_p b \) is rational. Then, \( \log_p b = r/q \) for some coprime \( r, q \in \mathbb{Z} \) with \( q \neq 0 \). Then,

\[ q \log_p b = r \implies (p^{\log_p b})^q = p^r \iff b^q = p^r \]

and since \( b \) is not a power of \( p \) it must be divisible by some other prime \( q \). Then \( q \divides p^r \), a contradiction since \( p \) is prime.

**Exercise 56.** We will work by contradiction.

Suppose there are only finitely many primes of the form \( 6k+5 \). Denote them \( p_0, p_1, \ldots, p_k \) and consider the number

\[ N = 6p_0p_1 \cdots p_k - 1. \]

Cleary \( N > 1 \) because \( p_0 = 5 \), so there exists a prime factor \( p \) dividing \( N \). We apply the division algorithm to divide \( p \) by 6 and obtain

\[ p = 6q + r, \quad r, q \in \mathbb{Z}, \quad 0 \leq r \leq 5. \]

We now divide into cases

1. Suppose \( r = 0, 2, 4 \); then \( p \) is even, i.e \( p = 2 \). Since \( 2 \divides N \) (it divides \( N + 1 \)) this is impossible; thus \( r \neq 0, 2, 4 \).
2. Suppose \( r = 3 \); then \( 3 \divides p \), i.e \( p = 3 \). Again, \( 3 \divides N \), a contradiction.
3. Suppose \( r = 5 \); thus \( p \) is of the form \( 6k+5 \) and by hypothesis we have \( p = p_i \) for some \( i \). Since \( p_i \divides N + 1 \) it does not divide \( N \), again a contradiction.
From these cases it follows that \( p \) is of the form \( 6k + 1 \). Since \( p \) is any prime factor of \( N \), we conclude that all the prime factors occurring in the prime factorization of \( N \) are of the form \( 6k + 1 \). In other words,
\[
N = \ell_1^{a_1} \cdots \ell_s^{a_s} \quad \text{with} \quad \ell_i = 6k_i + 1 \quad \text{distinct primes and} \quad a_i \geq 1.
\]
Note that \((6k + 1)(6k' + 1) = 6(6kk' + k + k') + 1\), that is the product of any two integers of the form \( 6k + 1 \) is also of this form. From the prime factorization above we conclude that \( N \) is of the form \( 6k + 1 \). This is incompatible with \( N \) being also of the form \( 6k - 1 \) as defined above. Thus our initial assumption is wrong, i.e. there are infinitely many primes of the form \( 6k + 5 \), as desired.

If you are familiar with congruences the last part of the proof can be restated as follows. From the cases it follows that any prime \( q \) dividing \( N \) is of the form \( 6a + 1 \), that is \( q \equiv 1 \pmod{6} \). Since the product of two such primes \( q_1, q_2 \) (not necessarily distinct) also satisfies \( q_1q_2 \equiv 1 \pmod{6} \) we conclude that \( N \equiv 1 \pmod{6} \) which is a contradiction with \( N \equiv -1 \equiv 5 \pmod{6} \).

Section 3.7

Exercise 2. We apply the theorem we learned in class to describe solutions of linear Diophantine equations.

a) The equation \( 3x + 4y = 7 \). Since \((3, 4) = 1 \mid 7 \) there are infinitely many solutions; note that \( x_0 = y_0 = 1 \) is a particular solution. Then all the solutions are of the form
\[
x = 1 + 4t, \quad y = 1 - 3t, \quad t \in \mathbb{Z}.
\]

b) The equation \( 12x + 18y = 50 \). Since \((12, 18) = 6 \mid 50 \) there are no solutions.

c) The equation \( 30x + 47y = -11 \). Clearly \((30, 47) = 1 \) (47 is prime) so there are solutions. We find a particular solution by applying the Euclidean algorithm followed by back substitution. Indeed,
\[
47 = 30 \cdot 1 + 17, \quad 30 = 17 \cdot 1 + 13, \quad 17 = 13 \cdot 1 + 4
\]
and
\[
13 = 4 \cdot 3 + 1, \quad 4 = 1 \cdot 4 + 0;
\]
in particular, this double-checks that \((30, 47) = 1\); we continue
\[
1 = 13 - 4 \cdot 3 = 13 - (17 - 13) \cdot 3 = 13 \cdot 4 - 17 \cdot 3 = (30 - 17) \cdot 4 - 17 \cdot 3 =
\]
\[
= 30 \cdot 4 - 17 \cdot 7 = 30 \cdot 4 - (47 - 30) \cdot 7 = 30 \cdot 11 - 47 \cdot 7.
\]
Thus \( x_1 = 11, \ y_1 = -7 \) is a particular solution to \( 30x + 47y = 1 \). Thus \( x_0 = -11x_1 = -121, \ y_0 = -11y_1 = 77 \) is a particular solution to the desired equation. Therefore, the general solution is given by
\[
x = -121 + 47t, \quad y = 77 - 30t, \quad t \in \mathbb{Z}.
\]

d) The equation \( 25x + 95y = 970 \). Since \((25, 95) = 5 \mid 970 \) there are infinitely many solutions. We divide both sides of the equation by 5 to obtain the equivalent equation
\[
5x + 19y = 194.
\]
Note that \((5, 19) = 1\) and \(x_1 = 4, y_1 = -1\) is a particular solution to \(5x + 19y = 1\); then \(x_0 = 194x_1 = 776, y_0 = 194y_1 = -194\) is a particular solution to our equation. Thus the general solution is given by
\[
x = 776 + 19t, \quad y = -194 - 5t, \quad t \in \mathbb{Z}.
\]

**e) The equation** \(102x + 1001y = 1\). We find \((102, 1001)\) by applying the Euclidean algorithm:
\[
1001 = 102 \cdot 9 + 83, \quad 102 = 83 \cdot 1 + 19, \quad 83 = 19 \cdot 4 + 7
\]
and
\[
19 = 7 \cdot 2 + 5, \quad 7 = 5 \cdot 1 + 2, \quad 5 = 2 \cdot 2 + 1,
\]

hence \((102, 1001) = 1\) and the equation has infinitely many solutions. We apply back substitution to find a particular solution:
\[
1 = 5 - 2 \cdot 2 = 5 - (7 - 5) \cdot 2 = 7 \cdot (-2) + 5 \cdot 3 = 7 \cdot (-2) + (19 - 7 \cdot 2) \cdot 3
\]
\[
= 19 \cdot 3 - 7 \cdot 8 = 19 \cdot 3 - (83 - 19 \cdot 4) \cdot 8 = 83 \cdot (-8) + 19 \cdot 35
\]
\[
= 83 \cdot (-8) + (102 - 83) \cdot 35 = 102 \cdot 35 - 83 \cdot 43 = 102 \cdot 35 - (1001 - 102 \cdot 9) \cdot 43
\]
\[
= 1001 \cdot (-43) + 102 \cdot 422.
\]
Thus \(x_0 = 422, y_0 = -43\) is a particular solution. Therefore, the general solution is given by
\[
x = 422 + 1001t, \quad y = -43 - 102t, \quad t \in \mathbb{Z}.
\]

**Exercise 6.** This problem can be stated as finding a non-negative solution to the Diophantine equation \(63x + 7 = 23y\), where \(x\) is the number of plantains in a pile, and \(y\) is the number of plantains each traveler receives.

Replace \(y\) by \(-y\) and rearrange the equation into \(63x + 23y = -7\) and note that \((63, 23) = 1\), hence there are infinitely many solutions. We apply Euclidean algorithm
\[
63 = 23 \cdot 2 + 17, \quad 23 = 17 \cdot 1 + 6, \quad 17 = 6 \cdot 2 + 5, \quad 6 = 5 \cdot 1 + 1
\]
and back substitution
\[
1 = 6 - 5 = 6 - (17 - 6 \cdot 2) = 6 \cdot 3 - 17 = (23 - 17) \cdot 3 - 17 =
\]
\[
= 23 \cdot 3 - 17 \cdot 4 = 23 \cdot 3 - (63 - 23 \cdot 2) \cdot 4 = 63 \cdot (-4) + 23 \cdot 11,
\]

hence \(x_1 = -4, y_0 = 11\) is a particular solution to \(63x + 23y = 1\). We conclude that \(x_0 = -7x_1 = 28, y_0 = -7y_1 = -77\) is a particular solution. Thus the general solution is given by
\[
x = 28 + 23t, \quad y = -77 - 63t, \quad t \in \mathbb{Z}.
\]
Replacing again \(y\) by \(-y\) we get the general solution to \(63x + 7 = 23y\) given by
\[
x = 28 + 23t, \quad y = 77 + 63t, \quad t \in \mathbb{Z}.
\]

These values of \(x, y\) are both positive when \(t \geq -1\), therefore the number of plantains in the pile could be any integer of the form \(28 + 23t\) for \(t \geq -1\).