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:
\[
\sum_{k=1}^{n+1} \frac{1}{k(k+1)} = \sum_{k=1}^{n} \frac{1}{k(k+1)} + \frac{1}{(n+1)(n+2)} = \frac{n}{n+1} + \frac{1}{(n+1)(n+2)} = \frac{n(n+2)}{(n+1)(n+2)} + \frac{1}{(n+1)(n+2)} = \frac{n^2 + 2n + 1}{(n+1)(n+2)} = \frac{n+1}{n+2},
\]
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
\[n - 6 = 7a + 10b\]
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

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

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

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

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.
Section 2.1

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 \( n \in \mathbb{Z}_{>0} \) 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 \( n \in \mathbb{Z}_{>0} \). Consider \( Q_n = n! + 1 \). There is a prime factor \( p | Q_n \). Suppose \( p \leq n \); then \( p | n! = n(n-1)(n-2)\ldots2\cdot1 \) therefore \( p | Q_n - n! = 1 \), 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 \( p | n! \), and so \( p | (n! - S_n) = 1 \), 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
\[
(i) \quad p | 2a \text{ implies } p = 2 \text{ or } p | a,
\]
(ii) \( p \mid 2b \) implies \( p = 2 \) or \( p \mid b \).

Suppose \( p 
eq 2 \). Then in (i) we have \( p \mid a \) and in (ii) we have \( p \mid b \); 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 \( d \mid a + b \) and \( d \mid a - b \) arguing as above we conclude that \( 2^k \mid 2a \) and \( 2^k \mid 2b \), that is
\[
2a = 2^k x \quad \text{and} \quad 2b = 2^k y
\]
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 \( 2 \mid a \) and \( 2 \mid b \), 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
\[
(a \pm b)(x \mp y) + (a - b)(x - y) = 2ax + 2by = 2(ax + by) = 2
\]
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.
Section 3.4

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

\[
(300,2160,5040) = ((300,2160),5040) = (60,5040) = 60.
\]

Section 3.5

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

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 \(a, b \in \mathbb{Z}_{>0}\). Suppose that
\[
(a, b) = 18 = 2 \cdot 3^2 \quad \text{and} \quad \text{LCM}(a, b) = 540 = 2^2 \cdot 3^3 \cdot 5.
\]
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,
\[
\min(d_2, e_2) = 1 \quad \text{max}(d_2, e_2) = 2.
\]
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 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
\[
a = p_1^{e_1} \cdots p_k^{e_k}, \quad b = p_1^{d_1} \cdots p_k^{d_k}, \quad e_i, d_i \geq 0
\]
(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,

\[
540 = 2^23^35 = LCM(a, b) = p_1^{\max(e_1, d_1)} \cdots p_k^{\max(e_k, d_k)},
\]
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

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

\[
5b^3 = (5k)^3 \iff b^3 = 5^2k^3 \implies 5 \mid b,
\]
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 \( q \mid p^r \), 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 \( p_0 = 5, p_1, \ldots, p_k \) and consider the number

\[
N = 6p_0p_1\cdots p_k - 1.
\]
Clearly \( N > 1 \) 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 \( 2 \mid N \) (it divides \( N + 1 \)) this is impossible; thus \( r \neq 0, 2, 4 \).
2. Suppose \( r = 3 \); then \( 3 \mid p \), i.e \( p = 3 \). Again, \( 3 \mid N \), 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 \( p_i \mid N + 1 \) 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 $(6k + 1)(6k' + 1) = 6(6k + k' + k') + 1$, 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

$$1 = 13 - 4 \cdot 3 = 13 - (17 - 3) \cdot 3 = 13 \cdot 4 - 17 \cdot 3 = (30 - 17) \cdot 4 - 17 \cdot 3 =$$

$$= 30 \cdot 4 - 17 \cdot 7 = 30 \cdot 4 - (47 - 30) \cdot 7 = 30 \cdot 11 - 47 \cdot 7.$$

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:
\[
1 = 5 \cdot 2 \cdot 2 = 5 \cdot (7 - 5) \cdot 2 = 7 \cdot (-2) + 5 \cdot 3 = 7 \cdot (-2) + (19 - 7 \cdot 2) \cdot 3 = 19 \cdot 3 \cdot 7 \cdot 8 = 19 \cdot 3 \cdot (83 - 19 \cdot 4) \cdot 8 = 83 \cdot (-8) + 19 \cdot 35 = 83 \cdot (-8) + (102 - 83) \cdot 35 = 102 \cdot 35 - 83 \cdot 43 = 102 \cdot 35 - (1001 - 102 \cdot 9) \cdot 43 = 1001 \cdot (-43) + 102 \cdot 422.
\]
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 \(t \geq -1\).
Exercise 4. Let \( a \in \mathbb{Z} \).

Suppose \( a \) is even; then \( a \equiv 0 \pmod{4} \) or \( a \equiv 2 \pmod{4} \). Since \( 0^2 = 0 \equiv 0 \pmod{4} \) and \( 2^2 = 4 \equiv 0 \pmod{4} \) we conclude \( a^2 \equiv 0 \pmod{4} \).

Suppose \( a \) is odd; then \( a \equiv 1 \pmod{4} \) or \( a \equiv 3 \pmod{4} \). Since \( 1^2 = 1 \equiv 1 \pmod{4} \) and \( 3^2 = 9 \equiv 1 \pmod{4} \) we conclude \( a^2 \equiv 1 \pmod{4} \).

Exercise 30. We will use induction to show that \( 4^n \equiv 1 + 3n \pmod{9} \) for all \( n \in \mathbb{Z}_{\geq 0} \).

Base \( n = 0 \): \( 4^0 = 1 \equiv 1 = 1 + 3 \cdot 0 \pmod{9} \).

Hypothesis: The result holds for \( n \).

Step \( n+1 \): We have

\[
4^{n+1} = 4 \cdot 4^n \equiv 4(1 + 3n) \equiv 4 + 12n \pmod{9}
\equiv 4 + 3n \equiv 1 + 3(n + 1) \pmod{9},
\]

as desired; we used the induction hypothesis in the first congruence.

Exercise 36. Note that the smallest power of 2 which is larger than all the exponents in this exercise is \( 2^8 = 256 \). Therefore, we will repeatedly square and reduce modulo 47 to compute \( 2^i \pmod{47} \) for \( 1 \leq i \leq 7 \). Indeed, we have

\[
\begin{align*}
2^1 &= 2 \equiv 2 \pmod{47} \\
2^2 &= 4 \equiv 4 \pmod{47} \\
2^4 &= 16 \equiv 16 \pmod{47} \\
2^8 &= 256 \equiv 21 \pmod{47} \\
2^{16} &= 21^2 \equiv 18 \pmod{47} \\
2^{32} &= 18^2 \equiv 42 \pmod{47} \\
2^{64} &= 42^2 \equiv 25 \pmod{47} \\
2^{128} &= 25^2 \equiv 14 \pmod{47}.
\end{align*}
\]

a) Compute \( 2^{32} \): We have seen above that \( 2^{32} \equiv 42 \pmod{47} \)

b) Compute \( 2^{47} \): Since \( 47 = 32 + 8 + 4 + 2 + 1 \), we have

\[
2^{47} = 2^{32}2^82^42^22^1 \equiv 42 \cdot 21 \cdot 16 \cdot 4 \cdot 2 \equiv 2 \pmod{47}.
\]

c) Compute \( 2^{200} \): Since \( 200 = 128 + 64 + 8 \), we have

\[
2^{200} = 2^{128}2^{64}2^8 \equiv 14 \cdot 25 \cdot 21 \equiv 18 \pmod{47}.
\]
**Exercise 2.** We will apply the theorem from class that fully describes the solutions of linear congruences.

a) **Solve** $3x \equiv 2 \pmod{7}$. Since $(3, 7) = 1$ there is exactly one solution mod 7. Since $3 \cdot 3 = 9 \equiv 2 \pmod{7}$ we conclude that $x \equiv 3 \pmod{7}$ is the unique solution of the congruences.

b) **Solve** $6x \equiv 3 \pmod{9}$. Since $(6, 9) = 3$ there are exactly three non-congruent solutions mod 9. Note that $x_0 \equiv 2 \pmod{9}$ is a particular solution; then $x \equiv 2 - (9/3)t = 2 - 3t$ with $0 \leq t \leq 2$ give all the non-congruent solutions. Indeed, $t = 0, 1, 2$ respectively correspond to the solutions $x \equiv 2, 8, 5 \pmod{9}$.

c) **Solve** $17x \equiv 14 \pmod{21}$. Since $(17, 21) = 1$ there is exactly one solution. We know that the solution will correspond to the $x$-coordinate of a particular solution of the Diophantine equation $17x - 21y = 14$. We compute it by applying the Euclidean algorithm and back substitution:

\[
21 = 17 \cdot 1 + 4, \quad 17 = 4 \cdot 4 + 1, \quad 4 = 4 \cdot 1 + 0
\]

and

\[
1 = 17 - 4 \cdot 4 = 17 - (21 - 17) \cdot 4 = 17 - 5 \cdot 21 - 5 \cdot 4,
\]

hence $x_1 = 5$, $y_1 = 4$ is a solution to $17x - 21y = 1$. Therefore, $x_0 = 14x_1 = 14 \cdot 5 = 70$, $y_0 = 14y_1 = 14 \cdot 4 = 56$ is a particular solution to $17x - 21y = 14$. It follows that $x \equiv x_0 \equiv 7 \pmod{21}$ is the unique solution to the congruence.

d) **Solve** $15x \equiv 9 \pmod{25}$. Since $(15, 25) = 5$ and $5 \nmid 9$ there are no solutions to the congruence.

**Exercise 6.** The congruence $12x \equiv c \pmod{30}$ has solutions if and only if $(12, 30) = 6$ divides $c$. In the range $0 \leq c < 30$ this occurs for $c = 0, 6, 12, 18, 24$ in which cases there are 6 non-congruent solutions.

**Exercise 8.** Since 13 is a small number we can solve this exercise by trial and error.

a) Since $7 \cdot 2 = 14 \equiv 1 \pmod{13}$ we have $2^{-1} \equiv 7 \pmod{13}$.

b) Since $9 \cdot 3 = 27 \equiv 1 \pmod{13}$ we have $3^{-1} \equiv 9 \pmod{13}$.

c) Since $8 \cdot 5 = 40 \equiv 1 \pmod{13}$ we have $5^{-1} \equiv 8 \pmod{13}$.

d) Since $6 \cdot 11 = 66 \equiv 1 \pmod{13}$ we have $11^{-1} \equiv 6 \pmod{13}$.

**Exercise 10.**

a) An integer $a$ will have an inverse mod 14 if and only if $ax \equiv 1 \pmod{14}$ has a solution, that is exactly when $(a, 14) = 1$. The numbers $a$ in the interval $1 \leq a \leq 14$ satisfying this condition are $\{1, 3, 5, 9, 11, 13\}$.

b) Note that the inverse of $a^{-1}$ is $a$ so the inverse of $a \in \{1, 3, 5, 9, 11, 13\}$ must also belong to this list since it contains all the invertible elements mod 14. Finally, note that

\[
1 \cdot 1 \equiv 1, \quad 3 \cdot 5 = 15 \equiv 1, \quad 9 \cdot 11 = 99 \equiv 1, \quad 13 \cdot 13 = 169 \equiv 1 \pmod{14}
\]

which means that

\[
1^{-1} \equiv 1, \quad 3^{-1} \equiv 5, \quad 5^{-1} \equiv 3 \pmod{14}
\]
and
\[ 9^{-1} \equiv 11, \quad 11^{-1} \equiv 9, \quad 13^{-1} \equiv 13 \pmod{14}. \]

**Section 4.3**

**Exercise 2.** The question is equivalent to find a solution to the congruences
\[ x \equiv 1 \pmod{2}, \quad x \equiv 1 \pmod{5}, \quad x \equiv 0 \pmod{3}. \]
The unique modulo 10 solution of the first two congruences is \( x \equiv 1 \pmod{10} \). Thus the original system is equivalent to
\[ x \equiv 1 \pmod{10}, \quad x \equiv 0 \pmod{3}. \]
We rewrite the first congruence as an equality, namely \( x = 1 + 10t \), where \( t \) is an integer. Inserting this expression for \( x \) into the second congruence, we find that
\[ 1 + 10t \equiv 0 \pmod{3} \iff t \equiv 2 \pmod{3}, \]
which means \( t = 2 + 3s \), where \( s \) is an integer. Hence any integer \( x = 1 + 10t = 1 + 10(2 + 3s) = 21 + 30s \) will be a solution to the problem. For example, taking \( s = 0 \) we get \( x = 21 \). In the language of congruences, we have shown that
\[ x \equiv 21 \pmod{30}, \]
is the unique solution mod 30.

We now solve this exercise by applying the CRT to the congruences
\[ x \equiv 1 \pmod{10}, \quad x \equiv 0 \pmod{3}. \]
Indeed, we have \( b_1 = 1, b_2 = 0, n_1 = 10, n_2 = 3, M = n_1n_2 = 30, M_1 = M/n_1 = 3 \) and \( M_2 = M/n_2 = 10; \) the formula for the unique solution modulo \( M \) gives
\[ x = b_1M_1y_1 + b_2M_2y_2 = 1 \cdot M_1 \cdot y_1 + 0 \cdot M_2 \cdot y_2 = 3y_1, \]
where \( y_1 \) satisfies \( M_1y_1 \equiv 1 \pmod{n_1} \), that is \( y_1 = 3^{-1} \pmod{10} = 7 \pmod{10} \). We conclude that
\[ x = 3 \cdot 7 = 21 \pmod{30}, \]
as expected.

**Exercise 4.** We will use the CRT.

a) Solve
\[ x \equiv 4 \pmod{11}, \quad x \equiv 3 \pmod{17}. \]
We have \((11, 17) = 1\). We have \( b_1 = 4, b_2 = 3, n_1 = 11, n_2 = 17, M = n_1n_2 = 187, M_1 = M/n_1 = 17 \) and \( M_2 = M/n_2 = 11; \) furthermore, we determine \( y_1, y_2 \) by solving the congruences \( M_iy_i \equiv 1 \pmod{n_i} \), that is
\[ 17y_1 \equiv 1 \pmod{11} \quad \text{and} \quad 11y_2 \equiv 1 \pmod{17}. \]
Both \( y_i \) can be found by solving the Diophantine equation \( 17y_1 + 11y_2 = 1 \). We only need a particular solution, and one is easy to find by trial and error: \( y_1 = 2, y_2 = -3 \). Now
\[ x = b_1 \cdot M_1 \cdot y_1 + b_2 \cdot M_2 \cdot y_2 = 4 \cdot 17 \cdot 2 + 3 \cdot 11 \cdot (-3) = 37. \]

Thus \( x = 37 \) is the unique solution modulo \( M = 187 \).
b) Note that 2, 3 and 5 are pairwise coprime. The first two equations can be rewritten as

\[ x \equiv -1 \pmod{2}, \quad x \equiv -1 \pmod{3} \]

and by the CRT they are equivalent to \( x \equiv -1 \pmod{6} \). Thus our system of congruences is equivalent to

\[ x \equiv -1 \pmod{6}, \quad x \equiv 3 \pmod{5}. \]

We have \( b_1 = -1, b_2 = 3, n_1 = 6, n_2 = 5, M = n_1 n_2 = 30, M_1 = M/n_1 = 5 \) and \( M_2 = M/n_2 = 6; \) furthermore, we easily find that

\[ y_1 = 5^{-1} \equiv -1 \pmod{6} \quad \text{and} \quad y_2 = 6^{-1} \equiv 1 \pmod{5}. \]

Thus by the formula for the unique solution is

\[ x \equiv (-1) \cdot 5 \cdot (-1) + 3 \cdot 6 \cdot 1 \equiv 23 \pmod{30}. \]

c) By looking at the congruences it is easy to see that \( x = 6 \) satisfies all of them. Thus by the CRT we have an unique solution \( x \equiv 6 \pmod{210} \), since \( 210 = 2 \cdot 3 \cdot 5 \cdot 7 \) and 2, 3, 5 and 7 are pairwise coprime.

Alternatively, we can apply the formula

\[ x \equiv 0 \cdot M_1 \cdot y_1 + 0 \cdot M_2 \cdot y_2 + 1 \cdot M_3 \cdot y_3 + 6 \cdot M_4 \cdot y_4 \pmod{210}, \]

where \( M_5 = 210/5 = 42 \) and \( M_4 = 210/7 = 30 \). To determine \( y_3 \), we solve \( 42y_3 \equiv 1 \pmod{5} \), or equivalently \( y_3 = 42^{-1} \equiv 2^{-1} \equiv 3 \pmod{5} \). To determine \( y_4 \), we solve \( 30y_4 \equiv 1 \pmod{7} \), or equivalently \( y_4 = 30^{-1} \equiv 2^{-1} \equiv 4 \pmod{7} \). Now \( x \equiv 1 \cdot 42 \cdot 3 + 6 \cdot 30 \cdot 4 \equiv 6 \pmod{210} \), as expected.

**Exercise 22.** If \( x \) is the number of gold coins, the problem is equivalent to finding the least positive solution to the following system of congruences:

\[ x \equiv 3 \pmod{17} \]
\[ x \equiv 10 \pmod{16} \]
\[ x \equiv 0 \pmod{15}. \]

As 17, 16, and 15 are pairwise coprime, we can use the CRT to find the unique solution modulo \( M = 15 \cdot 16 \cdot 17 = 4080 \). Thus the solution is given by the formula

\[ x \equiv 3 \cdot M_1 \cdot y_1 + 10 \cdot M_2 \cdot y_2 + 0 \cdot M_3 \cdot y_3 + 1 \cdot M_4 \cdot y_4 \pmod{M}, \]

where \( M_1 = 15 \cdot 16 = 240, M_2 = 15 \cdot 17 = 255, y_1 \) is a solution to the congruence

\[ (15 \cdot 16)y \equiv 1 \pmod{17} \iff (-2) \cdot (-1)y \equiv 2y \equiv 1 \pmod{17} \]

and \( y_2 \) is a solution to

\[ (15 \cdot 17)y \equiv 1 \pmod{16} \iff (-1) \cdot 1y \equiv -y \equiv 1 \pmod{16}. \]

Thus, we can take \( y_1 = 9 \) and \( y_2 = -1 \), obtaining

\[ x \equiv 3 \cdot 240 \cdot 9 + 10 \cdot 255 \cdot (-1) \equiv 3930 \pmod{4080}. \]

We conclude that, the number of coins can be \( 3930+4080n \) where \( n \) is a non-negative integer; the smallest such number is 3930.
Exercise 2.

a) The last 3 digits of 112250 are 250 which is divisible by $5^3 = 125$, but the last 4 digits are 2250 which is not divisible by $5^4 = 625$. Thus the largest power of 5 dividing 112250 is 3.

b) The last 4 digits of 4860625 are 0625 which is divisible by $5^4 = 625$, but the last 5 digits are 60625, which is not divisible by $5^5 = 3125$. Thus the largest power of 5 dividing 4860625 is 4.

c) The last 2 digits of 23555790 are 90 which is not divisible by $5^2 = 25$, but 23555790 is divisible by 5, so the largest power of 5 dividing 23555790 is 1.

d) The last 5 digits of 48126953125 are 53125 which is divisible by $5^5 = 3125$. Dividing 48126953125 by $5^5 = 3125$, we get 15400625. This number is divisible by 5 but not $5^5 = 3125$. Thus the highest power of 5 dividing 48126953125 is $5 + 4 = 9$.

Exercise 4. A number is divisible by 11 if and only if the integer formed by alternatively sum of its digits is divisible by 11. We use this to test divisibility.

a) 

$$1 - 0 + 7 - 6 + 3 - 7 + 3 - 2 = -1$$

so 10763732 is not divisible by 11.

b) 

$$1 - 0 + 8 - 6 + 3 - 2 + 0 - 0 + 1 - 5 = 0$$

so 1086320015 is divisible by 11.

c) 

$$6 - 7 + 4 - 3 + 1 - 0 + 9 - 7 + 6 - 3 + 7 - 5 = 8$$

so 674310976375 is not divisible by 11.

d) 

$$8 - 9 + 2 - 4 + 3 - 1 + 0 - 0 + 6 - 4 + 5 - 3 + 7 = 10$$

so 8924310064537 is not divisibly by 11.

Exercise 22. We know that the total cost being $x42y$ cents is divisible by 88 = 8·11 and so is divisible by both 11 and $2^3 = 8$. Thus 42y is divisible by $2^3 = 8$, and so 2y is divisible by $2^2 = 4$ and y is divisible by 2. The only number $0 \leq y < 10$ satisfying this is $y = 4$. As $x424$ is divisible by 11 we require that

$$x - 4 + 2 - 4 = x - 6$$

is divisible by 11. The only number $0 \leq x < 10$ satisfying this is $x = 6$. Thus the total cost was $64.24$ and each chicken cost $64.24/88 = $0.73.$
Section 5.5

Exercise 12. We use the fact that
\[ \sum_{i=1}^{10} ix_i \equiv 0 \pmod{11}. \]

a) We have
\[ 1 \cdot 0 + 2 \cdot 1 + 3 \cdot 9 + 4 \cdot 8 + 5 \cdot x_5 + 6 \cdot 3 + 7 \cdot 8 + 8 \cdot 0 + 9 \cdot 4 + 10 \cdot 9 \equiv 5x_2 + 8 \equiv 0 \pmod{11}. \]
Thus \( x_5 \equiv (-8) \cdot 5^{-1} \equiv 3 \cdot 9 \equiv 5 \pmod{11} \), and the missing digit is \( x_5 = 5 \).

b) We have
\[ 1 \cdot 9 + 2 \cdot 1 + 3 \cdot 5 + 4 \cdot 4 + 6 \cdot 2 + 7 \cdot 1 + 8 \cdot 2 + 9 \cdot x_9 + 10 \cdot 6 \equiv 9x_9 + 7 \equiv 0 \pmod{11}. \]
Thus \( x_9 \equiv (-7) \cdot 9^{-1} \equiv 4 \cdot 5 \equiv 9 \pmod{11} \), and the missing digit is \( x_9 = 9 \).

c) We have
\[ 1 \cdot x_1 + 2 \cdot 2 + 3 \cdot 6 + 4 \cdot 1 + 5 \cdot 0 + 6 \cdot 5 + 7 \cdot 0 + 8 \cdot 7 + 9 \cdot 3 + 10 \cdot 10 \equiv x_1 + 8 \equiv 0 \pmod{11}. \]
Thus \( x_1 \equiv -8 \equiv 3 \pmod{11} \), and the missing digit is \( x_1 = 3 \).

Exercise 13. Let \( x_i \) denote the digits of \( 0-07-289095-0 \) which is an ISBN10 code obtained by transposing two digits of a valid ISBN10 code. Let \( S \) denote the sum
\[ S = \sum_{i=1}^{10} ix_i = 3 \cdot 7 + 4 \cdot 2 + 5 \cdot 8 + 6 \cdot 9 + 7 \cdot 0 + 8 \cdot 9 + 9 \cdot 5 + 10 \cdot 0 \equiv 9 \pmod{11}, \]
hence \( S \not\equiv 0 \pmod{11} \) (as expected, since the code is invalid).
Let \( S' \) denote the sum corresponding to the original code. We have \( S' \equiv 0 \pmod{11} \). Suppose that the \( j \)th and \( k \)th digits were transposed. Then, to reconstruct \( S' \) from \( S \), we subtract the incorrectly positioned digits and add the correct ones, that is
\[ S' = S - jx_j - kx_k + jx_k + kx_j = S + (j - k)(x_k - x_j). \]
Now, \( S' \equiv S + (j - k)(x_k - x_j) \pmod{11} \) is equivalent to
\[ 0 \equiv 9 + (j - k)(x_k - x_j) \pmod{11} \iff (j - k)(x_k - x_j) \equiv -9 \pmod{11}. \]
By trial and error we find that this is satisfied by \( j = 7, k = 8 \) and no other cases. Thus the correct ISBN-10 is \( 0-07-289905-0 \).