Exercises

Chris J. Mitchell

8th December 2025

1 Questions

1.1 Chapter 1

1. On the subject of theorems and proofs, a simple theorem from geometry says that the area of any triangle is half the product of the length of the base times the height. Any side of the triangle can serve as the base. Can you prove this? You might find it easier to first think about a proof for a right angled triangle.

2. The three numbers $\{3, 4, 5\}$ form a Pythagorean triple. Can you find another Pythagorean triple other than triples of the form $\{3n, 4n, 5n\}$ for an integer n?

1.2 Chapter 2

1. If E is the set of even integers greater than zero, and S is the of squares (i.e. numbers which equal the square of a whole number), list the smallest three elements of $E \cap S$ and $E \cup S$.

2. Let $\sim$ be the relation, defined on the set of all people, where two people are related under $\sim$ if they share part of their name. So for example, Steve Smith $\sim$ Jamie Smith because they share the last name Smith. Similarly, Ravi Shastri $\sim$ Ravi Bopara since they both have the first name Ravi. Is $\sim$ an equivalence relation? If not, why not? That is, which properties of an equivalence relation does it satisfy and which doesn't it satisfy?

3. Give an example of two functions which when composed give the same answer either way round. Now give two functions which when composed in different orders give *different* results.

4. Define the operation Δ on pairs of integers to be the difference between them, where the difference is always zero or positive. So, for example, $4 \sim 7 = 3$ and $(-3) \sim 4 = 7$. Which of the four properties listed in Section 2.8, i.e. the existence of an identity element, the existence of an inverse, associativity and commutativity, does this operation satisfy? If it fails to possess a property, please give an example of where it fails.

1.3 Chapter 3

1. There is a simple partial ordering on the complex numbers ($\mathbb{C}$). What is it? However, this is not a total ordering — why?

2. Show by induction that the sum of the first n positive integers is $n(n+1)/2$.

3. Use the Euclidean algorithm to find the greatest common divisor of 462 and 1071.

4. The Collatz Conjecture was first formulated by German mathematician Lothar Collatz (1910-1990)[1] in 1937. The conjecture concerns the following function defined on the positive integers:

$$f(n) = \begin{cases} 3n+1 & \text{if } n \text{ is odd,} \\ n/2 & \text{if } n \text{ is even.} \end{cases}$$

   Suppose s is any positive integer — this is the 'starting value'. Define a sequence c_i by setting $c_1 = s$ and $c_{i+1} = f(c_i)$ for every $i \geq 1$. That is, recursively apply f to the starting value, and see what happens.

   The Collatz Conjecture states that, whatever the starting value s, the sequence will eventually reach 1. Although much has been proved about the sequences the function f generates, the conjecture remains unresolved, although it has been checked up to a very large number by computer. You might want to try a few small examples to convince yourself it is true.

   My question is the following. If $s = 27$, i.e. the starting value is 27, how long is it before you reach 1?

1.4 Chapter 4

1. In Chapter 4, I gave an example of computing a MOD11-2 check digit for the four-digit string 0749. What is the check digit for 0748?

[1] See, e.g., `https://mathshistory.st-andrews.ac.uk/Biographies/Collatz/`.

2. Find a number n such that $n \equiv 4 \pmod{6}$ and $n \equiv 1 \pmod{7}$. We know this number exists by the Chinese Remainder Theorem since 6 and 7 are coprime.

3. Suppose $p = 11$ and $q = 13$ are two primes to be used as part of an RSA key (this is a 'toy' example since in practice p and q will be many hundreds of decimal digits long). Then $n = pq = 143$, and $\phi(n) = (p-1)(q-1) = 120$. If the public encryption exponent is chosen to be 7, i.e. $e = 7$, then what is the private decryption exponent d?

1.5 Chapter 5

1. As I discussed in Chapter 5, $(\mathbb{Z}, +)$ is a group. Suppose I define a new operation on the integers , denoted by *, defined so that if a and b are integers,
$$a * b = a + b - 1.$$
Is $(\mathbb{Z}, *)$ a group? More specifically which properties of a group hold?

2. Does the group $(\mathbb{Z}_4, +)$ have a non-trivial subgroup, i.e. a subgroup other than the group itself and the subgroup consisting of just the identity element? If so, what is it?

3. Groups of order 2 and 3 are unique up to isomorphism, i.e. all groups of order 2 (and of order 3) are isomorphic to one another. Indeed this is always true for groups of prime order, since the only group of order p when p is prime is the cyclic group of that order. However, there is more than one group of order 4. How many are there and what are they?

4. Consider the following 'toy' example of Diffie-Hellman key agreement. Suppose we are working in the multiplicative group $(\mathbb{Z}_{23}^*, \times)$, a cyclic group of order 22 since $p = 23$ is prime. Note that $23 = 2 \times 11 + 1$, and 11 is prime, and so $(\mathbb{Z}_{23}^*, \times)$ has a cyclic subgroup of order 11. Also set $g = 2$ and it is straightforward to check that g has order 11, i.e. $2^{11} \equiv 1 \pmod{23}$ and $2^i \bmod 23 \neq 1$ for $1 \leq i < 11$.

   Now suppose A and B choose their private keys as $a = 6$ and $b = 15$ respectively. What secret key do they agree on after they have used the Diffie-Hellman protocol? Show that they both obtain the same secret key.

1.6 Chapter 6

1. Let S be any non-empty finite set, say $S = \{1, 2, \ldots, n\}$ for convenience. Let $\mathcal{S}$ be the set of all subsets of S. For example, if $n = 2$,

i.e. $S = \{1, 2\}$, then $\mathcal{S} = \{\emptyset, \{1\}, \{2\}, \{1, 2\}\}$. Show that $\mathcal{S}$ contains 2^n elements.

2. Building on the previous question, I need to introduce two operations on $\mathcal{S}$. If T and U are elements of $\mathcal{S}$, i.e. $T \subseteq S$ and $U \subseteq S$, then define:

   $$T + U = T \mathbin{\Delta} U$$

   and

   $$T \times U = T \cap U,$$

   where $T \mathbin{\Delta} U$ is what is known as the *symmetric difference* between T and U, containing all elements that are in either T or U, but not in both. So, for example, if $T = \{1, 2\}$ and $U = \{1, 3, 4\}$, then $T \mathbin{\Delta} U = \{2, 3, 4\}$.

   Now consider $(\mathcal{S}, +, \times)$. Does this form a commutative ring with one? More specifically which of the properties of a commutative ring with one are true?

3. The *Repetition Code* is a very simple example of a block code. If the symbols are 0 and 1, each block contains a single data bit, a say. If the block has length $n > 1$, then there are $n - 1$ check bits all set to a. That is, there are only two possible blocks, either all zeros or all ones. Decoding is simple — for every received block count the numbers of zeros and ones and choose the most common. What is the minimum distance of this code? If the code is used purely for error detection, how many errors in a block can it detect? If the code is used for error correction, how many errors in a block can it successfully correct?

1.7 Chapter 7

1. In Chapter 7 I described two versions of the division theorem — one version where the underlying ring $\mathcal{R} = (R, +, \cdot)$ is a commutative ring with one, and another version where the underlying ring is a field. These theorems state that if $f(x)$ and $g(x)$ are polynomials with coefficients from R, i.e. they are elements of $R[x]$, then there exist unique polynomials $q(x)$ and $r(x)$ such that

   $$f(x) = q(x) \cdot g(x) + r(x)$$

   where the degree of $r(x)$ is less than the degree of $g(x)$. As you might expect, $q(x)$ is known as the *quotient* and $r(x)$ is the *remainder*.

   In the commutative ring with one case, there is an additional restriction that $g(x)$ must be monic, i.e. it must have leading coefficient 1; this restriction disappears when $\mathcal{R}$ is a field.

Suppose $\mathcal{R} = (\mathbb{Z}, +, \cdot)$, i.e. the ring of integers. Give a simple example of why the restriction to monic polynomials $g(x)$ must apply in this case.

2. Consider the three stage shift register with characteristic polynomial $x^3 + x + 1$. If the first state of the register is 001, what will the successive states be? What period does the sequence of states have?

1.8 Chapter 8

1. In Chapter 4, I introduced integer modular arithmetic which allows for a ring to be defined. It is possible to define a modular version of other rings, such as the rational numbers $\mathbb{Q}$. Let $\mathbb{Q}_2$ contain all the non-negative rational numbers less than 2, where addition and multiplication work just as in $\mathbb{Q}$ but where an appropriate multiple of 2 is subtracted from the result to give a non-negative value less than 2. So, for example, $2 \times \frac{4}{3} = \frac{8}{3} \equiv \frac{2}{3}$ (by subtracting 2 from $\frac{8}{3}$).

   What properties does this structure have. Is $(\mathbb{Q}_2, +)$ a group? Is $(\mathbb{Q}_2^*, \times)$ a group? Indeed, is $(\mathbb{Q}_2, +, \times)$ a ring or even a field?

1.9 Chapter 9

1. Find a difference set other than $\{0, 1, 3\}$ modulo 7 or $\{0, 0, 2, 3, 4, 8\}$ modulo 11. Can you generate another difference set from $\{0, 1, 3\}$ modulo 7?

2 Answers

2.1 Chapter 1

1. The proof for a right angled triangle involves first imagining the triangle with the right angled corner at bottom left, with base length b and height h. Now take a second copy of the triangle and rotate it by 180 degrees. The two triangles can now be joined to form a b by h rectangle, which will clearly have area bh. Thus the triangle has area $\frac{bh}{2}$.

   A proof for a non-right-angled triangle works in a similar way. The two copies of the triangle can be joined to form a parallelogram, which with some surgery can be re-arranged to form a b by h rectangle.

2. Another triple is $\{5, 12, 13\}$. Euclid's formula states that any triple of numbers of the form $m^2 - n^2$, $2mn$, and $m^2 + n^2$ form a Pythagorean

triple if m and n are integers with $m \geq n$. Using the formula with $m = 2$ and $n = 1$ gives the triple $\{3, 4, 5\}$, and with $m = 3$ and $n = 1$ gives the triple $\{5, 12, 13\}$. Verifying that the formula works is straightforward.

2.2 Chapter 2

1. The smallest three elements of $E \cap S$ are 4, 16 and 36, and the smallest three elements of $E \cup S$ are 1, 2 and 4.

2. The relation $\sim$ is not an equivalence relation. It is reflexive and symmetric but not transitive. For example, Steve Waugh $\sim$ Steve Smith, and Steve Smith $\sim$ Jamie Smith, but Steve Waugh $\not\sim$ Jamie Smith.

3. Consider the two functions $f(x) = x + 1$ and $g(x) = x - 3$, then $g(f(x)) = (x + 1) - 3 = x - 2$ and $f(g(x)) = (x - 3) + 1 = x - 2$, i.e. in this particular case it follows that $f.g = g.f$. However, if you consider the two functions $f(x) = 2x$ and $g(x) = x^2$ defined on the reals, then $g(f(x)) = (2x)^2 = 4x^2$, whereas $f(g(x)) = 2(x^2) = 2x^2$. That is, $f.g$ is distinct from $g.f$. That is, in general, composition of functions is not commutative.

4. Three of the four properties hold, as follows.

   - There is an identity element, namely 0, since $x\Delta 0 = 0\Delta x = x$ for every integer x.
   - There is an inverse for every integer, since every integer is the inverse of itself, i.e. $x\Delta x = 0$ for every integer x.
   - However Δ is not associative, since, for example, $(1\Delta 2)\Delta 4 = 1\Delta 4 = 3$, whereas $1\Delta(2\Delta 4) = 1\Delta 2 = 1$.
   - It is commutative — this follows immediately from the definition.

2.3 Chapter 3

1. If $a + bi$ is a complex number, then define $|a + bi|$ to be $\sqrt{a^2 + b^2}$. This 'norm' function maps a complex number to a positive real number. If you think of complex numbers as being points on a plane, known as the *complex plane*, with the x axis being the 'real component' and the y axis being the 'imaginary' component, then the norm function has a simple geometric interpretation — it specifies the distance of the complex number from zero, i.e. the intersection of the x and y axes.

   I can now define a partial ordering using this norm function. If $a + bi$ and $c + di$ are two complex numbers, then say that $a + bi \leq c + di$ if and only if $|a+bi| \leq |c+di|$, where the ordering of the normed values is defined in the 'regular' way over the real numbers.

This is not a total ordering because there are infinitely many different complex numbers with the same norm (apart from zero). All the complex numbers that are the same distance from zero in the complex plane have the same norm. So, for example, $1+i$ has the same norm has $1-i$, $-1+i$ and $-1-i$.

2. The statement is true for $n = 1$, since the sum of the first single number is 1 and, when $n = 1$, $n(n+1)/2 = 1 \times 2/2 = 1$. Now suppose the statement is true for $n = k$ (for some $k \geq 1$), i.e. we know that the sum of the first k numbers is $k(k+1)/2$. We need to show that the statement is true for $n = k+1$. The sum of the first $k+1$ numbers is simply $k+1$ plus the sum of the first k numbers i.e.

$$(k+1) + \frac{k(k+1)}{2} = k+1+\frac{k^2+k}{2} = \frac{k^2+3k+2}{2} = \frac{(k+1)(k+2)}{2}.$$

That is, the statement holds for $n = k+1$ and the proof is complete.

3. The goal is to find the greatest common divisor of 462 and 1071. The Euclidean Algorithm works as follows.

   - $1071 = 2 \times 462 + 147$;
   - $462 = 3 \times 147 + 21$;
   - $147 = 7 \times 21 + 0$.

   That is, the greatest common divisor of 1071 and 462 is 21.

4. If $c_1 = 27$, then $c_{112} = 1$, and $c_i > 1$ for every smaller i. The sequence that results is sequence A008884 in the OEIS[2].

2.4 Chapter 4

1. I asked for the check digit for 0748. Following the same procedure as outlined in Chapter 4,, $a_5 = 0$, $a_4 = 7$, $a_3 = 4$ and $a_2 = 8$; to get the check digit I need to calculate a_1, using the following steps:

   - $S = a_5 = 0$;
   - $S \leftarrow (2S + a_4) \bmod 11 = 7 \bmod 11 = 7$;
   - $S \leftarrow (2S + a_3) \bmod 11 = 14 + 4 \bmod 11 = 7$;
   - $S \leftarrow (2S + a_2) \bmod 11 = 14 + 8 \bmod 11 = 0$.

   Finally set $a_1 = (1 - 2S) \bmod 11 = 1$, and so the check digit is 1.

[2] See `https://oeis.org/A008884`.

2. If $n = 22$, then $n \equiv 4 \pmod 6$ and $n \equiv 1 \pmod 7$. This is the only number less than $6 \times 7 = 42$ to satisfy these constraints since 6 and 7 are coprime.

3. The private decryption exponent must satisfy $de \equiv 1 \pmod{120}$, where $e = 7$. Finding d can be achieved easily using the Extended Euclidean Algorithm. First compute the greatest common divisor of 7 and 120, as follows:

   - $120 = 17 \times 7 + 1$;
   - $7 = 7 \times 1 + 0$.

   Working backwards we get $1 = 120 - 17 \times 7$, so $-17 \times 7 \equiv 1 \pmod{120}$. That is, $d \equiv -17 \equiv 103 \pmod{120}$. So $d = 103$.

2.5 Chapter 5

1. $(\mathbb{Z}, *)$ is a group. The identity element is 1, since $a * 1 = a + 1 - 1 = a$. The inverse of any element a is simply $2 - a$, since $a * (2 - a) = a + (2 - a) - 1 = 1$. The operation * is associative since $a * (b * c) = a + (b + c - 1) - 1 = a + b + c - 2 = (a + b - 1) + c - 1 = (a * b) * c$. It is in fact an abelian group.

2. Yes, $(\mathbb{Z}_4, +)$ does have a non-trivial subgroup. It is $(\{0, 2\}, +)$.

3. There are two non-isomorphic groups of order 4, namely the cyclic group of order 4, often written as C_4, and the cross-product of C_2, the cyclic group of order 2, with itself, i.e. $C_2 \times C_2$. Both of these are abelian. The reason there are no non-abelian groups of order 4 is simply because 4 is too small to contain the different values necessary. The smallest non-abelian group has order 6, and is the symmetric group S_3 of permutations of 3 elements. This is one of only two groups of order 6. For larger non-prime numbers, particularly those with many prime factors, the number of distinct groups grows fairly rapidly; for example, there are 5 non-isomorphic groups of order 8, 5 of order 12, and as many as 14 of order 16.

4. The example is in the multiplicative group $(\mathbb{Z}_{23}^*, \times)$ and $g = 2$. A and B choose their private keys as $a = 6$ and $b = 15$ respectively.

   The public key of $A = g^a = 2^6 = 64 \equiv 18 \pmod{23}$. The public key of $B = g^b = 2^{15} = 32768 \equiv 16 \pmod{23}$.

   A sends 18 (A's public key) to B who computes $18^{15} \equiv 4 \pmod{23}$. B sends 16 (B's public key) to A who computes $16^6 \equiv 4 \pmod{23}$.

   That is they both arrive at the secret key 4.

2.6 Chapter 6

1. We know that S contains n elements: $1, 2, \ldots, n$. Each of these elements can either be included in a subset or not; that is, working through the n elements one by one, there are $2 \times 2 \times \cdots \times 2$ possibilities for a subset, where there are n twos in the product. This is equal to 2^n, and the desired result follows.

2. Yes, this does form a special type of commutative ring with one, known as a *Boolean Ring* after the English mathematician, philosopher and logician George Boole (1815-1864)[3].

   The additive identity is the empty set, since $T \Delta \emptyset = T$ for any set T. Similarly, the multiplicative identity is the full set S, since $T \cap S = T$ for any subset T of S. The additive inverse of any set is the set itself, since $T \Delta T = \emptyset$ for any set T.

   Both addition and multiplication are commutative by definition. It remains to show associativity and distributivity. First observe that Δ is associative since an element is in $(T \Delta U) \Delta V$ if and only if it is in an odd number of the three sets T, U and V; exactly the same applies to elements of $T \Delta (U \Delta V)$. The fact that $\cap$ is associative is trivial to prove, since an element is in $(T \cap U) \cap V$ or equally in $T \cap (U \cap V)$ if and only if it is in all three of T, U and V.

   To show distributivity it is simplest to first introduce the notion of *set difference*. That is, if T and U are subsets of S, then the difference $T - U$ contains those elements of T that are not in U. It then follows that $T \Delta U = T \cup U - T \cap U$. This identity can then be used to easily establish distributivity, using the well-known rules to combine set union ($\cup$) and set intersection ($\cap$).

3. If the block length is n then the minimum distance is n — there are only two codewords and they differ in every bit position. A repetition code can be used to detect up to $n - 1$ errors in a block. If used for error correction then the code can be used to correct up to $\frac{n-1}{2}$ errors.

2.7 Chapter 7

1. Consider the two integer-coefficient polynomials $f(x) = x^3 + x - 1$ and $g(x) = 2x + 1$, observing that $g(x)$ is clearly not monic. It is impossible to 'divide' $f(x)$ by $g(x)$ since there is no integer multiple of 2, the leading term of $g(x)$, which equals 1, the leading term of $f(x)$. Of course, if $g(x) = x + 1$, which *is* monic, then the theorem works,

[3] See `https://mathshistory.st-andrews.ac.uk/Biographies/Boole/`.

and we have:

$$x^3 + x - 1 = (x^2 - x + 2)(x + 1) - 3$$

That is, in this case the quotient $q(x) = x^2 - x + 2$, and the remainder $r(x) = -3$. The degree of the remainder is -1, which is clearly less than 1, the degree of $g(x)$.

2. Since the shift register has characteristic polynomial $x^3 + x + 1$, there are feedbacks from the leftmost and the next to leftmost stages of the three, with their modulo 2 sum fed back into the rightmost of the three stages. If the first state of the register is 001, then the feedback bit is $0+0 = 0$, i.e. the next state is 010. The next feedback bit is $0+1 = 1$, and so the next state is 101. Continuing in this way, successive states are: 011, 111, 110, 100 and 001, i.e. we are back where we started. The period of the sequence of states is clearly 7, i.e. $2^3 - 1$. This follows since $x^3 + x + 1$ is primitive over $\mathbb{Z}_2$.

2.8 Chapter 8

1. It is straightforward to see that in $(\mathbb{Q}_2, +)$ the additive identity is 0, and addition is obviously commutative. The additive inverse of any element a is simply $2 - a$. Finally, addition is associative because it is in $(\mathbb{Q}, +)$, and so $(\mathbb{Q}_2, +)$ is an abelian group.

   However, things don't work so well for multiplication, i.e. for $(\mathbb{Q}_2^*, \cdot)$. There is a multiplicative identity, namely 1, and *some* elements have an inverse, i.e. those values x in the range $0.5 < x < 2$, since for such x it holds that $\frac{1}{x} < 2$. However, associativity of multiplication fails, and so $(\mathbb{Q}_2, \cdot)$ is not even a semigroup. To see why associativity fails consider the products $(\frac{3}{2} \times \frac{4}{3}) \times \frac{1}{2}$ and $\frac{3}{2} \times (\frac{4}{3} \times \frac{1}{2})$. It is simple to see that $(\frac{3}{2} \times \frac{4}{3}) \times \frac{1}{2} = 2 \times \frac{1}{2} = 0 \times \frac{1}{2} = 0$, whereas $\frac{3}{2} \times (\frac{4}{3} \times \frac{1}{2}) = \frac{3}{2} \times \frac{2}{3} = 1$.

   Moreover, the distributive law does not hold. To see this consider $\frac{1}{2} \cdot (1+1)=\frac{1}{2} \cdot 0 = 0$. If the distributive law held then this would equal $\frac{1}{2} \cdot 1 + \frac{1}{2} \cdot 1 = \frac{1}{2} + \frac{1}{2} = 1$, but $0 \neq 1$. Hence $(\mathbb{Q}_2, +, \cdot)$ is most certainly not a ring.

2.9 Chapter 9

1. There are infinitely many examples of difference sets other than those given in Chapter 9 — one example is $\{0, 1, 3, 9\}$ modulo 13. It is simple to generate another difference set from $\{0, 1, 3\}$ modulo 7 — just subtract every element from 7 to get $\{0, 4, 6\}$. It is also possible to add a constant to each element of a difference set to get another

difference set, e.g. by adding 2 to every element in $\{0, 1, 3\}$ we get the difference set $\{0 + 2, 1 + 2, 3 + 3\} = \{2, 3, 5\}$.