Discrete Mathematics

Exercises 1

Marcelo Fiore   Ohad Kammar   Dima Szamozvancev

1. On proofs

1.1. Basic exercises

The main aim is to practice the analysis and understanding of mathematical statements (e.g. by isolating the different components of composite statements) and exercise the art of presenting a logical argument in the form of a clear proof (e.g. by following proof strategies and patterns).

Prove or disprove the following statements.

1. Suppose n is a natural number larger than 2, and n is not a prime number. Then $2 \cdot n + 13$ is not a prime number.
2. If $x^2 + y = 13$ and $y \neq 4$ then $x \neq 3$.
3. For an integer n, n^2 is even if and only if n is even.
4. For all real numbers x and y there is a real number z such that $x + z = y - z$.
5. For all integers x and y there is an integer z such that $x + z = y - z$.
6. The addition of two rational numbers is a rational number.
7. For every real number x, if $x \neq 2$ then there is a unique real number y such that $2 \cdot y/(y+1) = x$.
8. For all integers m and n, if $m \cdot n$ is even, then either m is even or n is even.

1.2. Core exercises

Having practised how to analyse and understand basic mathematical statements and clearly present their proofs, the aim is to get familiar with the basics of divisibility.

1. Characterise those integers d and n such that:
   a) $0 \mid n$
   b) $d \mid 0$
2. Let k, m, n be integers with k positive. Show that:
$$(k \cdot m) \mid (k \cdot n) \iff m \mid n$$
3. Prove or disprove that: For all natural numbers n, $2 \mid 2^n$.
4. Show that for all integers l, m, n,
$$l \mid m \ \wedge \ m \mid n \implies l \mid n$$
5. Find a counterexample to the statement: For all positive integers k, m, n,
$$(m \mid k \ \wedge \ n \mid k) \implies (m \cdot n) \mid k$$

6. Prove that for all integers d, k, l, m, n,
   a) $d \mid m \wedge d \mid n \Longrightarrow d \mid (m+n)$
   b) $d \mid m \Longrightarrow d \mid k \cdot m$
   c) $d \mid m \wedge d \mid n \Longrightarrow d \mid (k \cdot m + l \cdot n)$
7. Prove that for all integers n,
$$30 \mid n \iff (2 \mid n \ \wedge \ 3 \mid n \ \wedge \ 5 \mid n)$$
8. Show that for all integers m and n,
$$(m \mid n \wedge n \mid m) \Longrightarrow (m = n \vee m = -n)$$
9. Prove or disprove that: For all positive integers k, m, n,
$$k \mid (m \cdot n) \Longrightarrow k \mid m \vee k \mid n$$
10. Let $P(m)$ be a statement for m ranging over the natural numbers, and consider the following derived statement (with n also ranging over the natural numbers):
$$P^{\#}(n) \triangleq \forall k \in \mathbb{N}.\ 0 \leq k \leq n \Longrightarrow P(k)$$
   a) Show that, for all natural numbers ℓ, $P^{\#}(\ell) \Longrightarrow P(\ell)$.
   b) Exhibit a concrete statement $P(m)$ and a specific natural number n for which the following statement *does not* hold:
$$P(n) \Longrightarrow P^{\#}(n)$$
   c) Prove the following:
      - $P^{\#}(0) \iff P(0)$
      - $\forall n \in \mathbb{N}.\ \big(P^{\#}(n) \Longrightarrow P^{\#}(n+1)\big) \iff \big(P^{\#}(n) \Longrightarrow P(n+1)\big)$
      - $\big(\forall m \in \mathbb{N}.\ P^{\#}(m)\big) \iff (\forall m \in \mathbb{N}.\ P(m))$

1.3. Optional exercises

1. A series of questions about the properties and relationship of triangular and square numbers (adapted from David Burton).
   a) A natural number is said to be *triangular* if it is of the form $\sum_{i=0}^{k} i = 0 + 1 + \cdots + k$, for some natural k. For example, the first three triangular numbers are $t_0 = 0$, $t_1 = 1$ and $t_2 = 3$.

      Find the next three triangular numbers t_3, t_4 and t_5.
   b) Find a formula for the k^{th} triangular number t_k.
   c) A natural number is said to be *square* if it is of the form k^2 for some natural number k.

Show that n is triangular iff $8 \cdot n + 1$ is a square. (Plutarch, circ. 100BC)

d) Show that the sum of every two consecutive triangular numbers is square. (Nicomachus, circ. 100BC)

e) Show that, for all natural numbers n, if n is triangular, then so are $9 \cdot n + 1$, $25 \cdot n + 3$, $49 \cdot n + 6$ and $81 \cdot n + 10$. (Euler, 1775)

f) Prove the generalisation: For all n and k natural numbers, there exists a natural number q such that $(2n + 1)^2 \cdot t_k + t_n = t_q$. (Jordan, 1991, attributed to Euler)

2. Let $P(x)$ be a predicate on a variable x and let Q be a statement not mentioning x. Show that the following equivalence holds:

$$\Big(\big(\exists x.\, P(x)\big) \Longrightarrow Q\Big) \iff \Big(\forall x.\, \big(P(x) \Longrightarrow Q\big)\Big)$$

Discrete Mathematics

Exercises 2

Marcelo Fiore   Ohad Kammar   Dima Szamozvancev

2. On numbers

2.1. Basic exercises

1. Let i, j be integers and let m, n be positive integers. Show that:
   a) $i \equiv i \pmod{m}$
   b) $i \equiv j \pmod{m} \implies j \equiv i \pmod{m}$
   c) $i \equiv j \pmod{m} \land j \equiv k \pmod{m} \implies i \equiv k \pmod{m}$
2. Prove that for all integers i, j, k, l, m, n with m positive and n nonnegative,
   a) $i \equiv j \pmod{m} \land k \equiv l \pmod{m} \implies i + k \equiv j + l \pmod{m}$
   b) $i \equiv j \pmod{m} \land k \equiv l \pmod{m} \implies i \cdot k \equiv j \cdot l \pmod{m}$
   c) $i \equiv j \pmod{m} \implies i^n \equiv j^n \pmod{m}$
3. Prove that for all natural numbers k, l and positive integers m,
   a) $\mathrm{rem}(k \cdot m + l, m) = \mathrm{rem}(l, m)$
   b) $\mathrm{rem}(k + l, m) = \mathrm{rem}(\mathrm{rem}(k, m) + l, m)$
   c) $\mathrm{rem}(k \cdot l, m) = \mathrm{rem}(k \cdot \mathrm{rem}(l, m), m)$
4. Let m be a positive integer.
   a) Prove the associativity of the addition and multiplication operations in $\mathbb{Z}_m$; that is:

   $$\forall i, j, k \in \mathbb{Z}_m.\ (i +_m j) +_m k = i +_m (j +_m k) \quad \text{and} \quad (i \cdot_m j) \cdot_m k = i \cdot_m (j \cdot_m k)$$

   b) Prove that the additive inverse of k in $\mathbb{Z}_m$ is $[-k]_m$.

2.2. Core exercises

1. Find an integer i, natural numbers k, l and a positive integer m for which $k \equiv l \pmod{m}$ holds while $i^k \equiv i^l \pmod{m}$ does not.
2. Formalise and prove the following statement: A natural number is a multiple of 3 iff so is the number obtained by summing its digits. Do the same for the analogous criterion for multiples of 9 and a similar condition for multiples of 11.
3. Show that for every integer n, the remainder when n^2 is divided by 4 is either 0 or 1.
4. What are $\mathrm{rem}(55^2, 79)$, $\mathrm{rem}(23^2, 79)$, $\mathrm{rem}(23 \cdot 55, 79)$ and $\mathrm{rem}(55^{78}, 79)$?
5. Calculate that $2^{153} \equiv 53 \pmod{153}$. At first sight this seems to contradict Fermat's Little Theorem, why isn't this the case though? *Hint:* Simplify the problem by applying known congruences to subexpressions using the properties in §2.1.2.

6. Calculate the addition and multiplication tables, and the additive and multiplicative inverses tables for $\mathbb{Z}_3$, $\mathbb{Z}_6$ and $\mathbb{Z}_7$.

7. Let i and n be positive integers and let p be a prime. Show that if $n \equiv 1 \pmod{p-1}$ then $i^n \equiv i \pmod{p}$ for all i not multiple of p.

8. Prove that $n^3 \equiv n \pmod{6}$ for all integers n.

9. Prove that $n^7 \equiv n \pmod{42}$ for all integers n.

2.3. Optional exercises

1. Prove that for all integers n, there exist natural numbers i and j such that $n = i^2 - j^2$ iff either $n \equiv 0 \pmod{4}$ or $n \equiv 1 \pmod{4}$ or $n \equiv 3 \pmod{4}$.

2. A *decimal* (respectively *binary*) *repunit* is a natural number whose decimal (respectively binary) representation consists solely of 1's.

   a) What are the first three decimal repunits? And the first three binary ones?

   b) Show that no decimal repunit strictly greater than 1 is a square, and that the same holds for binary repunits. Is this the case for every base? *Hint*: Use Lemma 27 of the notes.

Discrete Mathematics

Exercises 3

Marcelo Fiore Ohad Kammar Dima Szamozvancev

3. More on numbers

3.1. Basic exercises

1. Calculate the set $\mathrm{CD}(666, 330)$ of common divisors of 666 and 330.
2. Find the gcd of 21212121 and 12121212.
3. Prove that for all positive integers m and n, and integers k and l,
$$\gcd(m,n) \mid (k \cdot m + l \cdot n)$$
4. Find integers x and y such that $x \cdot 30 + y \cdot 22 = \gcd(30, 22)$. Now find integers x' and y' with $0 \leq y' < 30$ such that $x' \cdot 30 + y' \cdot 22 = \gcd(30, 22)$.
5. Prove that for all positive integers m and n, there exists integers k and l such that $k \cdot m + l \cdot n = 1$ iff $\gcd(m,n) = 1$.
6. Prove that for all integers n and primes p, if $n^2 \equiv 1 \pmod{p}$ then either $n \equiv 1 \pmod{p}$ or $n \equiv -1 \pmod{p}$.

3.2. Core exercises

1. Prove that for all positive integers m and n, $\gcd(m,n) = m$ iff $m \mid n$.
2. Let m and n be positive integers with $\gcd(m,n) = 1$. Prove that for every natural number k,
$$m \mid k \wedge n \mid k \iff m \cdot n \mid k$$
3. Prove that for all positive integers a, b, c, if $\gcd(a, c) = 1$ then $\gcd(a \cdot b, c) = \gcd(b, c)$.
4. Prove that for all positive integers m and n, and integers i and j:
$$n \cdot i \equiv n \cdot j \pmod{m} \iff i \equiv j \left(\mathrm{mod}\ \frac{m}{\gcd(m,n)}\right)$$
5. Prove that for all positive integers m, n, p, q such that $\gcd(m,n) = \gcd(p,q) = 1$, if $q \cdot m = p \cdot n$ then $m = p$ and $n = q$.
6. Prove that for all positive integers a and b, $\gcd(13 \cdot a + 8 \cdot b, 5 \cdot a + 3 \cdot b) = \gcd(a, b)$.
7. Let n be an integer.
    a) Prove that if n is not divisible by 3, then $n^2 \equiv 1 \pmod{3}$.
    b) Show that if n is odd, then $n^2 \equiv 1 \pmod{8}$.
    c) Conclude that if p is a prime number greater than 3, then $p^2 - 1$ is divisible by 24.

8. Prove that $n^{13} \equiv n \pmod{10}$ for all integers n.

9. Prove that for all positive integers l, m and n, if $\gcd(l, m \cdot n) = 1$ then $\gcd(l, m) = 1$ and $\gcd(l, n) = 1$.

10. Solve the following congruences:

    a) $77 \cdot x \equiv 11 \pmod{40}$

    b) $12 \cdot y \equiv 30 \pmod{54}$

    c) $\begin{cases} 13 \equiv z \pmod{21} \\ 3 \cdot z \equiv 2 \pmod{17} \end{cases}$

11. What is the multiplicative inverse of: (a) 2 in $\mathbb{Z}_7$, (b) 7 in $\mathbb{Z}_{40}$, and (c) 13 in $\mathbb{Z}_{23}$?

12. Prove that $\left[22^{12001}\right]_{175}$ has a multiplicative inverse in $\mathbb{Z}_{175}$.

3.3. Optional exercises

1. Let a and b be natural numbers such that $a^2 \mid b \cdot (b + a)$. Prove that $a \mid b$.

   Hint: For positive a and b, consider $a_0 = \frac{a}{\gcd(a,b)}$ and $b_0 = \frac{b}{\gcd(a,b)}$ so that $\gcd(a_0, b_0) = 1$, and show that $a^2 \mid b(b + a)$ implies $a_0 = 1$.

2. Prove the converse of §1.3.1(f): For all natural numbers n and s, if there exists a natural number q such that $(2n + 1)^2 \cdot s + t_n = t_q$, then s is a triangular number. (49th Putnam, 1988)

   Hint: Recall that if (†) $q = 2nk + n + k$ then $(2n + 1)^2\, t_k + t_n = t_q$. Solving for k in (†), we get that $k = \frac{q-n}{2n+1}$; so it would be enough to show that the fraction $\frac{q-n}{2n+1}$ is a natural number.

3. Informally justify the correctness of the following alternative algorithm for computing the gcd of two positive integers:

```
let rec gcd0(m, n) = if m = n then m
                     else let p = min m n
                          and q = max m n
                           in gcd0(p, q - p)
```

Discrete Mathematics

Exercises 4

Marcelo Fiore   Ohad Kammar   Dima Szamozvancev

4. On induction

4.1. Basic exercises

1. Prove that for all natural numbers $n \geq 3$, if n distinct points on a circle are joined in consecutive order by straight lines, then the interior angles of the resulting polygon add up to $180 \cdot (n-2)$ degrees.
2. Prove that, for any positive integer n, a $2^n \times 2^n$ square grid with any one square removed can be tiled with L-shaped pieces consisting of 3 squares.

4.2. Core exercises

1. Establish the following:
   (a) For all positive integers m and n,
   $$(2^n - 1) \cdot \sum_{i=0}^{m-1} 2^{i \cdot n} = 2^{m \cdot n} - 1$$
   (b) Suppose k is a positive integer that is not prime. Then $2^k - 1$ is not prime.
2. Prove that
   $$\forall n \in \mathbb{N}.\ \forall x \in \mathbb{R}.\ x \geq -1 \implies (1+x)^n \geq 1 + n \cdot x$$
3. Recall that the Fibonacci numbers F_n for $n \in \mathbb{N}$ are defined recursively by $F_0 = 0$, $F_1 = 1$, and $F_{n+2} = F_n + F_{n+1}$ for $n \in \mathbb{N}$.
   a) Prove Cassini's Identity: For all $n \in \mathbb{N}$,
   $$F_n \cdot F_{n+2} = {F_{n+1}}^2 + (-1)^{n+1}$$
   b) Prove that for all natural numbers k and n,
   $$F_{n+k+1} = F_{n+1} \cdot F_{k+1} + F_n \cdot F_k$$
   c) Deduce that $F_n \mid F_{l \cdot n}$ for all natural numbers n and l.
   d) Prove that $\mathtt{gcd}(F_{n+2}, F_{n+1})$ terminates with output 1 in n steps for all positive integers n.
   e) Deduce also that:
      (i) for all positive integers $n < m$, $\gcd(F_m, F_n) = \gcd(F_{m-n}, F_n)$,

      and hence that:

      (ii) for all positive integers m and n, $\gcd(F_m, F_n) = F_{\gcd(m,n)}$.

f) Show that for all positive integers m and n, $(F_m \cdot F_n) \mid F_{m \cdot n}$ if $\gcd(m,n) = 1$.

g) Conjecture and prove theorems concerning the following sums for any natural number n:

(i) $\sum_{i=0}^{n} F_{2 \cdot i}$

(ii) $\sum_{i=0}^{n} F_{2 \cdot i+1}$

(iii) $\sum_{i=0}^{n} F_i$

4.3. Optional exercises

1. Recall the `gcd0` function from §3.3.3. Use the Principle of Mathematical Induction from basis 2 to formally establish the following correctness property of the algorithm:

   For all natural numbers $l \geq 2$, we have that for all positive integers m, n, if $m + n \leq l$ then `gcd0`(m,n) terminates.

2. The set of *univariate polynomials* (over the rationals) on a variable x is defined as that of arithmetic expressions equal to those of the form $\sum_{i=0}^{n} a_i \cdot x^i$, for some $n \in \mathbb{N}$ and some *coefficients* $a_0, a_1, \ldots, a_n \in \mathbb{Q}$.

   (a) Show that if $p(x)$ and $q(x)$ are polynomials then so are $p(x) + q(x)$ and $p(x) \cdot q(x)$.

   (b) Deduce as a corollary that, for all $a, b \in \mathbb{Q}$, the linear combination $a \cdot p(x) + b \cdot q(x)$ of two polynomials $p(x)$ and $q(x)$ is a polynomial.

   (c) Show that there exists a polynomial $p_2(x)$ such that $p_2(n) = \sum_{i=0}^{n} i^2 = 0^2 + 1^2 + \cdots + n^2$ for every $n \in \mathbb{N}$.[1]

   Hint: Note that for every $n \in \mathbb{N}$,

   $$(n+1)^3 = \sum_{i=0}^{n}(i+1)^3 - \sum_{i=0}^{n} i^3$$

   (d) Show that, for every $k \in \mathbb{N}$, there exists a polynomial $p_k(x)$ such that, for all $n \in \mathbb{N}$, $p_k(n) = \sum_{i=0}^{n} i^k = 0^k + 1^k + \cdots + n^k$.

   Hint: Generalise the hint above, and the similar identity

   $$(n+1)^2 = \sum_{i=0}^{n}(i+1)^2 - \sum_{i=0}^{n} i^2$$

[1] Chapter 2.5 of *Concrete Mathematics* by R.L. Graham, D.E. Knuth and O. Patashnik looks at this in great detail.

Discrete Mathematics

Exercises 5

Marcelo Fiore   Ohad Kammar   Dima Szamozvancev

5. On sets

5.1. Basic exercises

1. Prove that $\subseteq$ is a partial order, that is, it is:

   a) reflexive: $\forall$ sets $A.\ A \subseteq A$

   b) transitive: $\forall$ sets $A, B, C.\ (A \subseteq B\ \wedge\ B \subseteq C) \Longrightarrow A \subseteq C$

   c) antisymmetric: $\forall$ sets $A, B.\ (A \subseteq B\ \wedge\ B \subseteq A) \iff A = B$

2. Prove the following statements:

   a) $\forall$ sets $A.\ \emptyset \subseteq A$

   b) $\forall$ sets $A.\ (\forall x.\ x \notin A) \iff A = \emptyset$

3. Find the union, and intersection of:

   a) $\{1, 2, 3, 4, 5\}$ and $\{-1, 1, 3, 5, 7\}$

   b) $\{x \in \mathbb{R} \mid x > 7\}$ and $\{x \in \mathbb{N} \mid x > 5\}$

4. Find the Cartesian product and disjoint union of $\{1, 2, 3, 4, 5\}$ and $\{-1, 1, 3, 5, 7\}$.

5. Let $I = \{2, 3, 4, 5\}$ and for each $i \in I$, let $A_i = \{i, i+1, i-1, 2 \cdot i\}$.

   a) List the elements of all sets A_i for $i \in I$.

   b) Let $\{A_i \mid i \in I\}$ stand for $\{A_2, A_3, A_4, A_5\}$. Find $\bigcup\{A_i \mid i \in I\}$ and $\bigcap\{A_i \mid i \in I\}$.

6. Let U be a set. For all $A, B \in \mathcal{P}(U)$, prove that:

   a) $A^c = B \iff (A \cup B = U\ \wedge\ A \cap B = \emptyset)$

   b) Double complement elimination: $(A^c)^c = A$

   c) The de Morgan laws: $(A \cup B)^c = A^c \cap B^c$ and $(A \cap B)^c = A^c \cup B^c$

5.2. Core exercises

1. Prove that for all for all sets U and subsets $A, B \subseteq U$:

   a) $\forall X.\ A \subseteq X\ \wedge\ B \subseteq X \iff (A \cup B) \subseteq X$ b) $\forall Y.\ Y \subseteq A\ \wedge\ Y \subseteq B \iff Y \subseteq (A \cap B)$

2. Either prove or disprove that, for all sets A and B,

   a) $A \subseteq B \Longrightarrow \mathcal{P}(A) \subseteq \mathcal{P}(B)$

   b) $\mathcal{P}(A \cup B) \subseteq \mathcal{P}(A) \cup \mathcal{P}(B)$

   c) $\mathcal{P}(A) \cup \mathcal{P}(B) \subseteq \mathcal{P}(A \cup B)$

d) $\mathcal{P}(A \cap B) \subseteq \mathcal{P}(A) \cap \mathcal{P}(B)$

e) $\mathcal{P}(A) \cap \mathcal{P}(B) \subseteq \mathcal{P}(A \cap B)$

3. Let U be a set. For all $A, B \in \mathcal{P}(U)$ prove that the following statements are equivalent.

   a) $A \cup B = B$ b) $A \subseteq B$ c) $A \cap B = A$ d) $B^c \subseteq A^c$

4. For sets A, B, C, D, prove or disprove at least three of the following statements:

   a) $(A \subseteq C \ \wedge\ B \subseteq D) \Longrightarrow A \times B \subseteq C \times D$

   b) $(A \cup C) \times (B \cup D) \subseteq (A \times B) \cup (C \times D)$

   c) $(A \times C) \cup (B \times D) \subseteq (A \cup B) \times (C \cup D)$

   d) $A \times (B \cup C) \subseteq (A \times B) \cup (A \times C)$

   e) $(A \times B) \cup (A \times D) \subseteq A \times (B \cup D)$

5. For sets A, B, C, D, prove or disprove at least three of the following statements:

   a) $(A \subseteq C \ \wedge\ B \subseteq D) \Longrightarrow A \uplus B \subseteq C \uplus D$

   b) $(A \cup B) \uplus C \subseteq (A \uplus C) \cup (B \uplus C)$

   c) $(A \uplus C) \cup (B \uplus C) \subseteq (A \cup B) \uplus C$

   d) $(A \cap B) \uplus C \subseteq (A \uplus C) \cap (B \uplus C)$

   e) $(A \uplus C) \cap (B \uplus C) \subseteq (A \cap B) \uplus C$

6. Prove the following properties of the big unions and intersections of a family of sets $\mathcal{F} \subseteq \mathcal{P}(A)$:

   a) $\forall U \subseteq A.\ (\forall X \in \mathcal{F}.\ X \subseteq U) \iff \bigcup \mathcal{F} \subseteq U$

   b) $\forall L \subseteq A.\ (\forall X \in \mathcal{F}.\ L \subseteq X) \iff L \subseteq \bigcap \mathcal{F}$

7. Let A be a set.

   a) For a family $\mathcal{F} \subseteq \mathcal{P}(A)$, let $\mathcal{U} \triangleq \{ U \subseteq A \mid \forall S \in \mathcal{F}.\ S \subseteq U \}$. Prove that $\bigcup \mathcal{F} = \bigcap \mathcal{U}$.

   b) Analogously, define the family $\mathcal{L} \subseteq \mathcal{P}(A)$ such that $\bigcap \mathcal{F} = \bigcup \mathcal{L}$. Also prove this statement.

5.3. Optional advanced exercises

1. Prove that for all families of sets $\mathcal{F}_1$ and $\mathcal{F}_2$,

$$\left(\bigcup \mathcal{F}_1\right) \cup \left(\bigcup \mathcal{F}_2\right) = \bigcup (\mathcal{F}_1 \cup \mathcal{F}_2)$$

   State and prove the analogous property for intersections of non-empty families of sets.

2. For a set U, prove that $(\mathcal{P}(U), \subseteq, \cup, \cap, U, \emptyset, (\cdot)^c)$ is a Boolean algebra.

Discrete Mathematics

Exercises 6

Marcelo Fiore   Ohad Kammar   Dima Szamozvancev

6. On relations

6.1. Basic exercises

1. Let $A = \{1, 2, 3, 4\}$, $B = \{a, b, c, d\}$ and $C = \{x, y, z\}$.
   Let $R = \{(1, a), (2, d), (3, a), (3, b), (3, d)\} : A \nrightarrow B$
   and $S = \{(b, x), (b, y), (c, y), (d, z)\} : B \nrightarrow C$.

   Draw the internal diagrams of the relations. What is the composition $S \circ R : A \nrightarrow C$?

2. Prove that relational composition is associative and has the identity relation as the neutral element.

3. For a relation $R : A \nrightarrow B$, let its *opposite*, or *dual relation*, $R^{\mathrm{op}} : B \nrightarrow A$ be defined by:

   $$b \, R^{\mathrm{op}} \, a \iff a \, R \, b$$

   For $R, S : A \nrightarrow B$ and $T : B \nrightarrow C$, prove that:

   a) $R \subseteq S \implies R^{\mathrm{op}} \subseteq S^{\mathrm{op}}$

   b) $(R \cap S)^{\mathrm{op}} = R^{\mathrm{op}} \cap S^{\mathrm{op}}$

   c) $(R \cup S)^{\mathrm{op}} = R^{\mathrm{op}} \cup S^{\mathrm{op}}$

   d) $(T \circ S)^{\mathrm{op}} = S^{\mathrm{op}} \circ T^{\mathrm{op}}$

6.2. Core exercises

1. Let $R, R' \subseteq A \times B$ and $S, S' \subseteq B \times C$ be two pairs of relations and assume $R \subseteq R'$ and $S \subseteq S'$. Prove that $S \circ R \subseteq S' \circ R'$.

2. Let $\mathcal{F} \subseteq \mathcal{P}(A \times B)$ and $\mathcal{G} \subseteq \mathcal{P}(B \times C)$ be two collections of relations from A to B and from B to C, respectively. Prove that

   $$\left(\bigcup \mathcal{G}\right) \circ \left(\bigcup \mathcal{F}\right) = \bigcup \{ S \circ R \mid R \in \mathcal{F}, S \in \mathcal{G} \} : A \nrightarrow C$$

   Recall that the notation $\{ S \circ R : A \nrightarrow C \mid R \in \mathcal{F}, S \in \mathcal{G} \}$ is common syntactic sugar for the formal definition $\{ T \in \mathcal{P}(A \times C) \mid \exists R \in \mathcal{F}.\ \exists S \in \mathcal{G}.\ T = S \circ R \}$. Hence,

   $$T \in \{ S \circ R \in A \nrightarrow C \mid R \in \mathcal{F}, S \in \mathcal{G} \} \iff \exists R \in \mathcal{F}.\ \exists S \in \mathcal{G}.\ T = S \circ R$$

   What happens in the case of big intersections?

3. Suppose R is a relation on a set A. Prove that

   a) R is reflexive iff $\mathrm{id}_A \subseteq R$

   b) R is symmetric iff $R = R^{\mathrm{op}}$

c) R is transitive iff $R \circ R \subseteq R$

d) R is antisymmetric iff $R \cap R^{\mathrm{op}} \subseteq \mathrm{id}_A$

4. Let R be an arbitrary relation on a set A, for example, representing an undirected graph. We are interested in constructing the smallest transitive relation (graph) containing R, called the *transitive closure* of R.

   a) We define the family of relations which are transitive supersets of R:

   $$\mathcal{T}_R \triangleq \{\, Q\colon A \nrightarrow A \mid R \subseteq Q \text{ and } Q \text{ is transitive} \,\}$$

   R is not necessarily going to be an element of this family, as it might not be transitive. However, R is a *lower bound* for $\mathcal{T}_R$, as it is a subset of every element of the family.

   Prove that the set $\bigcap \mathcal{T}_R$ is the transitive closure for R.

   b) $\bigcap \mathcal{T}_R$ is the intersection of an infinite number of relations so it's difficult to compute the transitive closure this way. A better approach is to start with R, and keep adding the missing connections until we get a transitive graph. This can be done by repeatedly composing R with itself: after n compositions, all paths of length n in the graph represented by R will have a transitive connection between their endpoints.

   Prove that the (at least once) iterated composition $R^{\circ+} \triangleq R \circ R^{\circ*}$ is the transitive closure for R, i.e. it coincides with the greatest lower bound of $\mathcal{T}_R$: $R^{\circ+} = \bigcap \mathcal{T}_R$. *Hint*: show that $R^{\circ+}$ is both an element and a lower bound of $\mathcal{T}_R$.

7. On partial functions

7.1. Basic exercises

1. Let $A_2 = \{\,1, 2\,\}$ and $A_3 = \{\,a, b, c\,\}$. List the elements of the sets $\mathrm{PFun}(A_i, A_j)$ for $i, j \in \{\,2, 3\,\}$. *Hint*: there may be quite a few, so you can think of ways of characterising all of them without giving an explicit listing.
2. Prove that a relation $R\colon A \nrightarrow B$ is a partial function iff $R \circ R^{\mathrm{op}} \subseteq \mathrm{id}_B$.
3. Prove that the identity relation is a partial function, and that the composition of partial functions is a partial function.

7.2. Core exercises

1. Show that $(\mathrm{PFun}(A, B), \subseteq)$ is a partial order. What is its least element, if it exists?
2. Let $\mathcal{F} \subseteq \mathrm{PFun}(A, B)$ be a non-empty collection of partial functions from A to B.

   a) Show that $\bigcap \mathcal{F}$ is a partial function.

   b) Show that $\bigcup \mathcal{F}$ need not be a partial function by defining two partial functions $f, g : A \rightharpoonup B$ such that $f \cup g : A \nrightarrow B$ is a non-functional relation.

   c) Let $h\colon A \rightharpoonup B$ be a partial function. Show that if every element of $\mathcal{F}$ is below h then $\bigcup \mathcal{F}$ is a partial function.

8. On functions

8.1. Basic exercises

1. Let $A_2 = \{1,2\}$ and $A_3 = \{a,b,c\}$. List the elements of the sets $\mathrm{Fun}(A_i, A_j)$ for $i, j \in \{2,3\}$.
2. Prove that the identity partial function is a function, and the composition of functions yields a function.
3. Prove or disprove that $(\mathrm{Fun}(A,B), \subseteq)$ is a partial order.
4. Find endofunctions $f, g : A \to A$ such that $f \circ g \neq g \circ f$.

8.2. Core exercises

1. A relation $R : A \nrightarrow B$ is said to be *total* if $\forall a \in A.\ \exists b \in B.\ a\,R\,b$. Prove that this is equivalent to $\mathrm{id}_A \subseteq R^{\mathrm{op}} \circ R$. Conclude that a relation $R : A \nrightarrow B$ is a function iff $R \circ R^{\mathrm{op}} \subseteq \mathrm{id}_B$ and $\mathrm{id}_A \subseteq R^{\mathrm{op}} \circ R$.
2. Let $\chi : \mathcal{P}(U) \to (U \Rightarrow [2])$ be the function mapping subsets $S \subseteq U$ to their characteristic functions $\chi_S : U \to [2]$.
   a) Prove that for all $x \in U$,
      - $\chi_{A\cup B}(x) = (\chi_A(x) \vee \chi_B(x)) = \max(\chi_A(x), \chi_B(x))$
      - $\chi_{A\cap B}(x) = (\chi_A(x) \wedge \chi_B(x)) = \min(\chi_A(x), \chi_B(x))$
      - $\chi_{A^c}(x) = \neg(\chi_A(x)) = (1 - \chi_A(x))$

   b) For what construction $A?B$ on sets A and B does it hold that

   $$\chi_{A?B}(x) = (\chi_A(x) \oplus \chi_B(x)) = (\chi_A(x) +_2 \chi_B(x))$$

   for all $x \in U$, where $\oplus$ is the *exclusive or* operator? Prove your claim.

8.3. Optional advanced exercise

Consider a set A together with an element $a \in A$ and an endofunction $f : A \to A$.

Say that a relation $R : \mathbb{N} \nrightarrow A$ is (a,f)-*closed* whenever

$$R(0,a) \quad \text{and} \quad \forall n \in \mathbb{N}, x \in A.\ R(n,x) \Longrightarrow R(n+1, f(x))$$

Define the relation $F : \mathbb{N} \nrightarrow A$ as

$$F \triangleq \bigcap \{ R : \mathbb{N} \nrightarrow A \mid R \text{ is } (a,f)\text{-closed} \}$$

a) Prove that F is (a,f)-closed.

b) Prove that F is total, that is: $\forall n \in \mathbb{N}.\ \exists y \in A.\ F(n,y)$.

c) Prove that F is a function $\mathbb{N} \to A$, that is: $\forall n \in \mathbb{N}.\ \exists! y \in A.\ F(n,y)$.

   Hint: Proceed by induction. Observe that, in view of the previous item, to show that $\exists! y \in A.\ F(k,y)$ it suffices to exhibit an (a,f)-closed relation R_k such that $\exists! y \in A.\ R_k(k,y)$. (Why?) For instance, as the relation $R_0 = \{(m,y) \in \mathbb{N} \times A \mid m = 0 \Longrightarrow y = a\}$ is (a,f)-closed one has that $F(0,y) \Longrightarrow R_0(0,y) \Longrightarrow y = a$.

d) Show that if h is a function $\mathbb{N} \to A$ with $h(0) = a$ and $\forall n \in \mathbb{N}.\ h(n+1) = f(h(n))$ then $h = F$.

Thus, for every set A together with an element $a \in A$ and an endofunction $f : A \to A$ there exists a unique function $F : \mathbb{N} \to A$, typically said to be *inductively defined*, satisfying the recurrence relation

$$F(n) = \begin{cases} a & \text{for } n = 0 \\ f(F(n-1)) & \text{for } n \geq 1 \end{cases}$$

Discrete Mathematics

Exercises 7

Marcelo Fiore   Ohad Kammar   Dima Szamozvancev

9. On bijections

9.1. Basic exercises

1. a) Define a function that has (i) none, (ii) exactly one, and (iii) more than one retraction.

   b) Define a function that has (i) none, (ii) exactly one, and (iii) more than one section.

2. Let n be an integer.

   a) How many sections are there for the absolute-value map $x \mapsto |x| : [-n..n] \to [0..n]$?

   b) How many retractions are there for the exponential map $x \mapsto 2^x : [0..n] \to [0..2^n]$?

3. Give an example of two sets A and B and a function $f : A \to B$ such that f has a retraction but no section. Explain how you know that f has these properties.

4. Prove that the identity function is a bijection and that the composition of bijections is a bijection.

5. For $f : A \to B$, prove that if there are $g, h : B \to A$ such that $g \circ f = \mathrm{id}_A$ and $f \circ h = \mathrm{id}_B$ then $g = h$. Conclude as a corollary that, whenever it exists, the inverse of a function is unique.

9.2. Core exercises

1. We say that two functions $s : A \to B$ and $r : B \to A$ are a *section-retraction pair* whenever $r \circ s = \mathrm{id}_A$; and that a function $e : B \to B$ is an *idempotent* whenever $e \circ e = e$. This question demonstrates that section-retraction pairs and idempotents are closely connected: any section-retraction pair gives rise to an idempotent function, and any idempotent function can be split into a section-retraction pair.

   a) Let $f : C \to D$ and $g : D \to C$ be functions such that $f \circ g \circ f = f$.

      (i) Can you conclude that $f \circ g$ is idempotent? What about $g \circ f$? Justify your answers.

      (ii) Define a map g' using f and g that satisfies both

      $$f \circ g' \circ f = f \qquad \text{and} \qquad g' \circ f \circ g' = g'$$

   b) Show that if $s : A \to B$ and $r : B \to A$ are a section-retraction pair then the composite $s \circ r : B \to B$ is idempotent.

   c) Show that for every idempotent $e : B \to B$ there exists a set A (called a *retract* of B) and a section-rectraction pair $s : A \to B$ and $r : B \to A$ such that $s \circ r = e$.

10. On equivalence relations

10.1. Basic exercises

1. Prove that the isomorphism relation $\cong$ between sets is an equivalence relation.
2. Prove that the identity relation id_A on a set A is an equivalence relation, and that $A/\mathrm{id}_A \cong A$.
3. Show that, for a positive integer m, the relation $\equiv_m$ on $\mathbb{Z}$ given by

$$x \equiv_m y \iff x \equiv y \pmod{m}$$

   is an equivalence relation. What are the equivalence classes of this relation?
4. Show that the relation $\equiv$ on $\mathbb{Z} \times \mathbb{Z}^+$ given by

$$(a, b) \equiv (x, y) \iff a \cdot y = x \cdot b$$

   is an equivalence relation. What are the equivalence classes of this relation?

10.2. Core exercises

1. Let E_1 and E_2 be two equivalence relations on a set A. Either prove or disprove the following statements.
   a) $E_1 \cup E_2$ is an equivalence relation on A.
   b) $E_1 \cap E_2$ is an equivalence relation on A.
2. For an equivalence relation E on a set A, show that $[a_1]_E = [a_2]_E$ iff $a_1 \, E \, a_2$, where

$$[a]_E = \{ x \in A \mid x \, E \, a \}.$$

3. For a function $f : A \to B$ define a relation $\equiv_f$ on A by the rule: for all $a, a' \in A$,

$$a \equiv_f a' \iff f(a) = f(a')$$

   a) Show that for every function $f : A \to B$, the relation $\equiv_f$ is an equivalence relation on A.
   b) Prove that every equivalence relation E in a set A is equal to $\equiv_q$, where $q : A \twoheadrightarrow A/E$ is the quotient function $q(a) = [a]_E$.
   c) Prove that for every surjection $f : A \twoheadrightarrow B$,

$$B \cong \big(A/\equiv_f\big)$$

Discrete Mathematics

Exercises 8

Marcelo Fiore   Ohad Kammar   Dima Szamozvancev

11. On surjections and injections

11.1. Basic exercises

1. Give two examples of functions that are surjective, and two examples of functions that are not.

2. Give two examples of functions that are injective, and two examples of functions that are not.

11.2. Core exercises

1. Explain and justify the phrase *injections can be undone*.

2. Show that $f : A \to B$ is a surjection if and only if for all sets C and functions $g, h\colon B \to C$, $g \circ f = h \circ f$ implies $g = h$.

   What would be an analogous condition for injections?

12. On images

12.1. Basic exercises

1. Let $R_2 = \{\, (m,n) \mid m = n^2 \,\}\colon \mathbb{N} \nrightarrow \mathbb{Z}$ be the integer square-root relation. What is the direct image of $\mathbb{N}$ under R_2? And what is the inverse image of $\mathbb{N}$?

2. For a relation $R\colon A \nrightarrow B$, show that:

   a) $\overrightarrow{R}(X) = \bigcup_{x\in X} \overrightarrow{R}(\{\, x \,\})$ for all $X \subseteq A$

   b) $\overleftarrow{R}(Y) = \left\{\, a \in A \,\middle|\, \overrightarrow{R}(\{\, a \,\}) \subseteq Y \,\right\}$ for all $Y \subseteq B$.

12.2. Core exercises

1. For $X \subseteq A$, prove that the direct image $\overrightarrow{f}(X) \subseteq B$ under an injective function $f : A \rightarrowtail B$ is in bijection with X; that is, $X \cong \overrightarrow{f}(X)$.

2. Prove that for a surjective function $f : A \twoheadrightarrow B$, the direct image function $\overrightarrow{f} : \mathcal{P}(A) \to \mathcal{P}(B)$ is surjective.

3. Show that any function $f : A \to B$ can be decomposed into an injection and a surjection: that is, there exists a set X, a surjection $s\colon A \twoheadrightarrow X$ and an injection $i\colon X \rightarrowtail B$ such that $f = i \circ s$.

4. For a relation $R\colon A \nrightarrow B$, prove that

   a) $\overrightarrow{R}\left(\bigcup \mathcal{F}\right) = \bigcup\left\{\, \overrightarrow{R}(X) \,\middle|\, X \in \mathcal{F} \,\right\}$ for all $\mathcal{F} \subseteq \mathcal{P}(A)$

   b) $\overleftarrow{R}\left(\bigcap \mathcal{G}\right) = \bigcap\left\{\, \overleftarrow{R}(Y) \,\middle|\, Y \in \mathcal{G} \,\right\}$ for all $\mathcal{G} \subseteq \mathcal{P}(B)$

5. Show that, by the inverse image, every map $A \to B$ induces a *Boolean algebra map* $\mathcal{P}(B) \to \mathcal{P}(A)$. That is, for every function $f : A \to B$, its inverse image preserves set operations:

- $\overleftarrow{f}(\emptyset) = \emptyset$
- $\overleftarrow{f}(B) = A$
- $\overleftarrow{f}(X \cup Y) = \overleftarrow{f}(X) \cup \overleftarrow{f}(Y)$
- $\overleftarrow{f}(X \cap Y) = \overleftarrow{f}(X) \cap \overleftarrow{f}(Y)$
- $\overleftarrow{f}(X^{\mathrm{c}}) = \left(\overleftarrow{f}(X)\right)^{\mathrm{c}}$

13. On countability

13.1. Basic exercises

1. Prove that every finite set is countable.
2. Demonstrate that $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ are countable sets.

13.2. Core exercises

1. Let A be an infinite subset of $\mathbb{N}$. Show that $A \cong \mathbb{N}$. *Hint*: Adapt the argument shown in the proof of Proposition 168, showing that the map $\mathbb{N} \to A$ is both injective and surjective.
2. For an infinite set A, prove that the following are equivalent:
   a) There is a bijection $\mathbb{N} \xrightarrow{\cong} A$.
   b) There is a surjection $\mathbb{N} \twoheadrightarrow A$.
   c) There is an injection $A \rightarrowtail \mathbb{N}$.
3. Prove that:
   a) Every subset of a countable set is countable.
   b) The product and disjoint union of countable sets is countable.
4. For a set A, prove that there is no injection $\mathcal{P}(A) \rightarrowtail A$.

13.3. Optional advanced exercise

1. Prove that if A and B are countable sets then so are A^*, $\mathcal{P}_{\mathrm{fin}}(A)$ and $\mathrm{PFun}_{\mathrm{fin}}(A, B)$.