Caution: The notation $[n]$ can denote both the set of numbers $\{1, \ldots, n\}$ or the equivalence class of n with respect to some equivalence relation. Which of these is meant should be clear from context. On this sheet, it will be *mostly* mean the latter, since we talk about equivalence relations. But to clear up the ambiguity, we mostly explicitly wrote either $\{1, \ldots, n\}$ or $[n]_\sim$ in the solutions.

Exercise 1

a) Give two relations each over the set [5]:
   i) that are well-founded
   ii) that are not well-founded

b) Which of the following relations is well-founded? Give a justification of why or why not.
   i) A relation that is irreflexive, asymmetric, and finite.
   ii) The relation $R = \{(n-1, n) \mid n \in \mathbb{N}\}$.
   iii) The relation RR, where R is defined as above.
   v) The divisibility order on $\mathbb{N}$, i.e. $R = \{(a, b) \mid a, b \in \mathbb{N} \text{ and } \exists c(c \in \mathbb{Z} \wedge a \cdot c = b)\}$.
   vi) The relation $\{(uabv, ubav) \mid u, v \in \{a, b, c\}^*\}$; that is, two words w and w' are related if we can obtain w' from w by replacing one occurrence of the subword ab with ba.

Note: Exercise iv) was removed because the supposed partial order in it was not actually a partial order.

Solution:

a) i) As long as the transitive closure of the relation defined over the set [5] does not contain any cycles, it will be well founded in this case because the set [5] is finite. E.g. $R_1 = \emptyset$, $R_2 = \{(1, 2), (2, 3), (3, 5)\}$.
   ii) An infinite descending chain must be present in the relation to make it not well founded. E.g. in $R_3 = \{(1, 2), (2, 3), (3, 5), (5, 1)\}$, we have the infinite descending chain $1, 2, 3, 5, 1, 2, 3, 5, 1, \ldots$. Another trivial example is $R_4 = [5] \times [5]$.

b) i) Such a relation is not necessarily well-founded as it may contain cycles. The above example of $R = \{(1, 2), (2, 3), (3, 5), (5, 1)\}$ is irreflexive, asymmetric, and finite but it still contains an infinite descending chain.
   ii) Well-founded. If we start at n, we can descend at most $n + 1$ times as the relation is only defined on $\mathbb{N}$; it is not defined past -1.
   iii) Well-founded. This relation is similar to the example above, but now it can be written as $R = \{(n-2, n) \mid n \in \mathbb{N}\}$. Since we now take two steps at a time, we can only make $\lceil \frac{n}{2} \rceil$. In general, it is easy to see that if R is well-founded then R^n is also well-founded for any $n \geq 1$.
   v) Well-founded. If we start at a non-zero number n, then every time we descend, the numbers get strictly smaller and we already know that $<\mathbb{N}$ is well-founded, so we can only descend finitely often also in the divisibility order (at most $n - 1$ times since 1 is least).

If we start at 0, we can descend to any number $n \in \mathbb{N} \setminus \{0\}$ and then we can again only descend at most $n-1$ times, as we have just seen.

Note that this is an interesting case: for any natural number n, there is a descending chain in the divisibility order starting from 0. So there are arbitrarily long infinite descending chains, but there is no *infinite* descending chain.

vi) Well-founded. Every time we descend, we replace a ba in the word with ab while leaving the rest of the word the same. So if we had an infinite descending chain $w_0, w_1, w_2, \ldots$ with $|w_0| = n$ then this would also be an infinite descending chain in the n-times lexicographic product of the (obviously well-founded) relation $a \prec b \prec c$, and the lexicographic product of finitely many well-founded relations is again well-founded.

An alternative view is that we can define a 'measure' function $m : \Sigma^* \to \mathbb{N}$ that counts the number of index pairs (i, j) with $1 \leq i < j \leq |w|$ such that $w_i = b$ and $w_j = a$. Every time we descend, this measure function decreases by 1, so it is clear that we can only descend finitely often (namely $m(w_0)$ times).

Exercise 2
For each of the following, determine if it is an equivalence relation or not. If yes, also describe what the equivalence classes look like.

a) $x \sim y$ iff $x + y$ is odd (over the set $\mathbb{Z}$)
b) $x \sim y$ iff $x + y$ is even (over the set $\mathbb{N}$)
c) $x \sim y$ iff $|x - y| \leq 5$ (over the set $\mathbb{Z}$)
d) $x \sim y$ iff $f(x) = f(y)$ (over the set A) for some function $f : A \to B$
e) $x \sim_z y$ for points $x, y \in \mathbb{R}^2$ iff x and y have the same distance from some fixed point $z \in \mathbb{R}^2$
f) $l_1 \sim l_2$ iff l_1 and l_2 are parallel lines in the Euclidean plane
g) $l_1 \sim l_2$ iff l_1 and l_2 are orthogonal lines in the Euclidean plane
h) $l_1 \sim l_2$ iff l_1 and l_2 are intersecting lines in the Euclidean plane

Solution:

a) No. This not even reflexive since $x + x = 2x$ is never odd. (Transitivity also does not hold, e.g. $1 \sim 2$ and $2 \sim 3$ but $1 \nsim 3$.

b) Yes. Reflexive since $x + x = 2x$ is always even. Symmetric due to commutativity of $+$. Transitive because if $x+y$ is even then x and y are either both odd or both even. If additionally $y + z$ is even, then in the first case z also has to be even and in the second case it also has to be odd.

The two equivalence classes are simply the set of all even numbers $[0]_\sim$ and the set of all odd numbers $[1]_\sim$.

c) No. It is reflexive and symmetric, but transitivity is violated because $0 \sim 3$ and $3 \sim 6$ but $0 \nsim 6$.

d) Yes. Reflexivity, symmetric, and transitivity are all obvious. The equivalence classes are all of the form $f^{-1}(y)$ for some $y \in \operatorname{ran}(f)$. We have $[x]_\sim = f^{-1}(f(x))$.

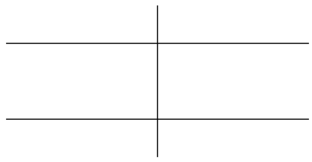
The equivalence classes of $\sim$ are also called the *fibres* of f. The equivalence relation $\sim$ is sometimes called the *equivalence kernel.*

e) Yes. This is just an instance of d) with the function $x \mapsto d(x, z)$ where $d(\cdot, \cdot)$ denotes the distance in the Euclidean plane. The equivalence classes of $\sim$ are circles around the point z. Each real number $r \geq 0$ gives rise to an equivalence that is a circle of radius r around z.

f) Yes. Reflexivity, symmetry, and transitivity are easy to see, and the equivalence classes are simply bundles of parallel lines (i.e. lines that face in the same direction). Every angle between 0° (inclusive) and 360° (exclusive) gives rise to a different equivalence class.

g) No. This already violates reflexivity since no line is orthogonal to itself.

h) No. This violates transitivity. In the following configuration, each of the horizontal lines intersects with the vertical one, but the two horizontal lines do not intersect.



Exercise 3

For $m \in \mathbb{Z}$, define a relation $\equiv_m$ on $\mathbb{Z}$ defined such that $a \equiv_m b \leftrightarrow m \mid (a - b)$.

You may use without proof that if $a \mid b$ and $a \mid c$ then also $a \mid -a$ and $a \mid (b + c)$.

a) Show that $\equiv_m$ is an equivalence relation.

b) What do the equivalence classes of $\equiv_4$ look like? What about $\equiv_m$ in general (for $m \geq 2$)?

c) What are the equivalence classes of $\equiv_0$ and $\equiv_1$?

d) Let $f, g : \mathbb{Z}/{\equiv_m} \times \mathbb{Z}/{\equiv_m} \to \mathbb{Z}/{\equiv_m}$ with $f([x], [y]) = [x + y]$ and $g([x], [y]) = [x \cdot y]$.
Show that f and g are well-defined.

e) What would be a reasonable canonical representative of the equivalence class $[a]_{\equiv_m}$ for $m \geq 2$?

Solution:

a)
- Reflexivity: $a \equiv_m a$ because $m \mid 0 = (a - a)$.
- Symmetry: Suppose $a \equiv_m b$. Then $m \mid (a - b)$. But then also $m \mid -(a - b) = b - a$ and thus $b \equiv_m a$.
- Transitivity: Suppose $a \equiv_m b$ and $b \equiv_m c$. Then $m \mid (a - b)$ and $m \mid (b - c)$. But then also $m \mid (a - b) + (b - c) = (a - c)$.

b)
- $[0]_{\equiv_4} = \{\ldots, -8, -4, 0, 4, 8, \ldots\}$
- $[1]_{\equiv_4} = \{\ldots, -7, -3, 1, 5, 9, \ldots\}$
- $[2]_{\equiv_4} = \{\ldots, -6, -2, 2, 6, 10, \ldots\}$
- $[3]_{\equiv_4} = \{\ldots, -5, -1, 3, 7, 11, \ldots\}$

In general, the equivalence classes have the form $[a]_{\equiv_m} = \{\ldots, a - 2m, a - m, a, a + m, a + 2m, \ldots\}$.

c)
- $a \equiv_0 b \quad \leftrightarrow \quad 0 \mid (a - b) \quad \leftrightarrow \quad a - b = 0 \quad \leftrightarrow \quad a = b$
So $a \equiv_0 b$ is simply the identity relation, whose equivalence classes have the form $[a]_0 = \{a\}$.
- $a \equiv_1 b \quad \leftrightarrow \quad 1 \mid (a - b) \quad \leftrightarrow \quad$ True
Thus $a \equiv_1 b$ is simply the universal relation $\mathbb{Z} \times \mathbb{Z}$ and there is only one big equivalence class, namely $\mathbb{Z}$ itself.

d)
- We need to prove that the function $(a, b) \mapsto [a+b]_{\equiv_m}$ is invariant under $\equiv_m$. That is: if $a \equiv_m a'$ and $b \equiv_m b'$, then $[a+b]_{\equiv_m} = [a'+b']_{\equiv_m}$, i.e. $a + b \equiv_m a' + b'$.

  Unfolding the definition of $\equiv_m$ everywhere, we have as assumptions $m \mid (a - a')$ and $m \mid (b - b')$ and we must show that $m \mid ((a + b) - (a' + b'))$. We can rearrange this goal to $m \mid ((a - a') + (b - b'))$, which follows directly from the assumptions.

- We shorten things a bit this time: Suppose $m \mid (a - a')$ and $m \mid (b - b')$. Obtain $k, l \in \mathbb{Z}$ such that $a - a' = km$ and $b - b' = lm$, i.e. $a' = a - km$ and $b' = b - lm$.

  We need to show that $m \mid (a \cdot b - a' \cdot b')$. We simplify the right-hand side by plugging in the above equations for a' and b' and obtain:

  $$a \cdot b - a' \cdot b' = ab - (a - km)(b - lm) = m(al + bk - kl)$$

  This is now obviously divisible by m, as required.

e) One can e.g. simply pick the smallest non-negative number in the equivalence class. This can be computed as $a - \lfloor \frac{a}{m} \rfloor \cdot m$, i.e. the remainder of the integer division $a \div m$ (this remainder is often written as 'a mod b', or, in many programming languages, '$a \,\%\, b$').

Bonus exercise

Let $\sim_1$ and $\sim_2$ be equivalence relations on some set A. We say that $\sim_1$ is a *refinement* of $\sim_2$ if $x \sim_1 y$ implies $x \sim_2 y$ for all $x, y \in A$. We write this as $\sim_1 \preceq \sim_2$.

a) Check that $\preceq$ defines a partial order on the set of equivalence relations.

b) List all equivalence relations (or equivalently, partitions) of the set $\{1, 2, 3, 4\}$ in a format of your choice and draw the the refinement relation on these as a Hasse diagram.

c) In general, what are the finest and coarsest equivalence relations on A, i.e. what are the least and greatest elements of $\preceq$? What do their equivalence classes look like?

d) Show that $\sim_1 \preceq \sim_2$ iff every equivalence class of $\sim_1$ is a subset of an equivalence class of $\sim_2$.

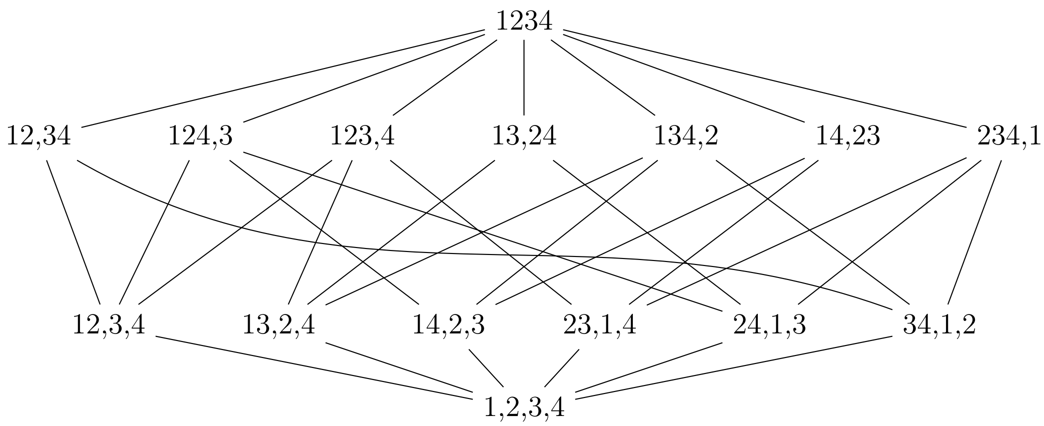
e) Write a computer program that generates a list of all equivalence relations on the set $\{1, \ldots, n\}$ in a format of your choice. How many are there for $n = 0$ to 10?

Solution:

a) All three properties are fairly obvious:
- Reflexivity: $x \sim_1 y$ implies $x \sim_1 y$ for all $x, y \in A$.
- Antisymmetry: If $\sim_1 \preceq \sim_2$ and $\sim_2 \preceq \sim_1$ then for any $x, y \in A$ we have $x \sim_1 y \to x \sim_2 y$ and $x \sim_2 y \to x \sim_1 y$, so $x \sim_1 y \leftrightarrow x \sim_2 y$, so $\sim_1 = \sim_2$.
- Transitivity: If $\sim_1 \preceq \sim_2$ and $\sim_2 \preceq \sim_3$ then for any $x, y \in A$ with $x \sim_1 y$ we have $x \sim_2 y$ and then $x \sim_3 y$.

b) We simply write out the equivalence classes and abbreviate a bit, e.g. we write $12, 34$ instead of $\{\{1, 2\}, \{3, 4\}\}$. We then have the following 15 equivalence relations, grouped by how many equivalence classes there are and what size they have:
- four different classes: $1, 2, 3, 4$
- one class of size 2 and two classes of size 1: $12, 3, 4$, $13, 2, 4$, $14, 2, 3$, $23, 1, 4$, $24, 1, 3$, $34, 1, 2$
- two classes of size 2: $12, 34$, $13, 24$, $14, 23$
- one class of size 3, one class of size 1: $123, 4$, $124, 3$, $134, 2$, $234, 1$

- only one class: 1234



c) The finest one (least element of $\preceq$) is the discrete relation (or identity relation) Id_A where every element is its own equivalence class.

The coarsest one (greatest element of $\preceq$) is the universal relation $A \times A$ with only one big equivalence class, namely A itself.

d) For the first direction, suppose $\sim_1 \preceq \sim_2$ and let X be an equivalence class of $\sim_1$. Then there exists $x \in A$ such that $X = [x]_{\sim_1}$. We then claim that $[x]_{\sim_1} \subseteq [x]_{\sim_2}$. To show this, let $y \in [x]_{\sim_1}$. Then $y \sim_1 x$. But then also $y \sim_2 x$ by our assumption and thus $y \in [x]_{\sim_2}$.

For the other direction, suppose every equivalence class of $\sim_1$ is a subset of some equivalence class of $\sim_2$. We need to show that $\sim_1 \preceq \sim_2$. So let $x, y \in A$ with $x \sim_1 y$. Then $y \in [x]_{\sim_1}$. But then by our assumption there exists some $z \in A$ with $[x]_{\sim_1} \subseteq [z]_{\sim_2}$ and thus $x \in [z]_{\sim_2}$ and also $y \in [z]_{\sim_2}$ and thus $x \sim_2 z$ and $y \sim_2 z$. By transitivity, $x \sim_2 y$ as desired.

e) The function `partitions` computes a list of all partitions of the input set S. We shall represent sets as lists with no duplicate elements. A partition is represented as a set of sets (i.e. a list of lists). Note that since we represent the input S as a list, we have some implicit order on the elements (i.e. there is a 'first element').

If S is empty, the empty partition is the only partition.

Otherwise, we pick the first element x of S and then construct an equivalence class for it. Every subset of S that contains x is a valid choice, so we just pick an arbitrary subset X of $S \setminus \{x\}$, and use $X \cup \{x\}$ as the equivalence class of x.

Then we recursively find a partition of the remaining set $S \setminus (X \cup \{x\})$.

```haskell
import Data.List

type Partition a = [[a]]

partitions :: Eq a => [a] -> [Partition a]
partitions [] = [[]]
partitions (x : xs) =
    [(x : ys) : cs | ys <- subsequences xs, cs <- partitions (xs \\ ys)]
```

Note that due to the way we construct these partitions, there are no duplicate elements in the result list.

Denote the number of equivalence relations on $\{1, \ldots, n\}$ with B_n With a simple

```
map (\n -> length $ partitions [1..n]) [0..10]
```

we can compute B_n for $n = 0$ to 10:

n	0	1	2	3	4	5	6	7	8	9	10
B_n	1	1	2	5	15	52	203	877	4,140	21,147	115,975

These are the so-called *Bell numbers* (A000110 on OEIS).