

## Exam topics

1. Basic structures: sets, lists, functions
  - (a) Sets  $\{ \}$ : write all elements, or define by condition
  - (b) Set operations:  $A \cup B$ ,  $A \cap B$ ,  $A \setminus B$ ,  $A^c$
  - (c) Lists  $( )$ : Cartesian product  $A \times B$
  - (d) Functions  $f : A \rightarrow B$  defined by any input-output rule
  - (e) Injective function:  $\forall a_1, a_2 \in A: a_1 \neq a_2 \Rightarrow f(a_1) \neq f(a_2)$
  - (f) Surjective function:  $\forall b \in B, \exists a \in A$  with  $f(a) = b$
  - (g)  $A, B$  have same cardinality: there is a bijection  $f : A \rightarrow B$
  - (h)  $A$  is countable: there is a bijection  $f : \mathbb{N} \rightarrow A$
2. Formal logic
  - (a) Statements: definitely true or false
  - (b) Conditional (open) statement  $P(x)$ : true/false depends on variable  $x$
  - (c) Logical operations: *and, or, not, implies*
  - (d) Truth tables and logical equivalence
  - (e) Implication  $P \Rightarrow Q$  equivalent to: contrapositive  $\text{not}(Q) \Rightarrow \text{not}(P)$ ;  
independent from: converse  $Q \Rightarrow P$ ; inverse  $\text{not}(P) \Rightarrow \text{not}(Q)$
  - (f) Negate implication:  $\text{not}(P \Rightarrow Q)$  is equivalent to:  $P$  and  $\text{not}(Q)$
  - (g) Quantifiers:  $\forall$  for all,  $\exists$  there exists;
  - (h) Negate quantifiers:  $\text{not}(\forall x, P(x))$  is equivalent to:  $\exists x, \text{not}(P(x))$
  - (i) Logical equivalences and set equations
  - (j) Logic in mathematical language versus everyday language
3. Methods of proof (can be combined)
  - (a) Direct proof
  - (b) Proof by cases
  - (c) Proof of the contrapositive
  - (d) Proof by contradiction
  - (e) Proof by induction (also complete induction)
4. Axioms of a Group  $(G, *)$  (All variables below mean elements of  $G$ .)
  - (a) Closure:  $a * b \in G$ .
  - (b) Associativity:  $(a * b) * c = a * (b * c)$
  - (c) Identity: There is  $e$  with  $e * a = a$  and  $a * e = a$  for all  $a$ .
  - (d) Inverses: For each  $a$ , there is some  $b$  with  $a * b = e$  and  $b * a = e$ .
 Extra axioms
  - (e) Commutativity:  $a * b = b * a$ .
  - (f) Distributivity of times over plus:  $a \cdot (b + c) = a \cdot b + a \cdot c$  and  $(b + c) \cdot a = b \cdot a + c \cdot a$ .
5. Divisibility of integers (All variables below mean integers.)
  - (a) Divisibility:  $a|b$  means  $b = ac$  for some  $c \in \mathbb{Z}$

- (b) Properties of divisibility:
- $a | b, c \implies a | mb + nc$  for all  $m, n$
  - $a | b$  and  $b | c \implies a | c$ .
  - $a | b$  and  $b | a \implies a = \pm b$ .
- (c) Prime and composite
- Test:  $a$  is composite  $\implies a$  has prime factor  $p \leq \sqrt{a}$ .
- (d) Greatest common divisor  $\gcd(a, b)$ ; relatively prime means  $\gcd(a, b) = 1$ .
- (e) Division Lemma:  $a = qb + r$  with remainder  $0 \leq r < b$ .
- (f) Euclidean Algorithm computes remainders  $a > b > r_1 > \dots > r_k > 0$ .
- Computes  $\gcd(a, b) = r_k$ .
  - Finds  $m, n$  with  $\gcd(a, b) = ma + nb$ .
- (g) Consequences of  $\gcd(a, b) = ma + nb$
- Find integer solutions  $(x, y)$  to equation  $ax + by = c$ , if  $\gcd(a, b) | c$ .
  - If  $e | a$  and  $e | b$ , then  $e | \gcd(a, b)$ .
  - Euclid's Lemma: If  $c | ab$  and  $\gcd(c, a) = 1$ , then  $c | b$ .
  - Prime Lemma: If  $p$  is prime with  $p | ab$ , then  $p | a$  or  $p | b$ .
  - For  $\bar{a} \in \mathbb{Z}_n$ , find multiplicative inverse  $\bar{b} = \bar{a}^{-1}$ , i.e.  $ab \equiv 1 \pmod{n}$ .
- (h) Fundamental Theorem of Arithmetic
- $n > 1$  is a product of primes uniquely, except for rearranging factors.
  - There is a unique list of powers  $s_1, s_2, s_3, \dots \geq 0$  with:  $n = 2^{s_1} 3^{s_2} 5^{s_3} 7^{s_4} 11^{s_5} \dots$ .
6. Equivalence relation  $\cong$  on a set  $S$
- (a) Defining properties:
- Reflexive:  $a \cong a$
  - Symmetric: If  $a \cong b$ , then  $b \cong a$ .
  - Transitive: If  $a \cong b$  and  $b \cong c$ , then  $a \cong c$
- (b) Equivalence class  $[a] = \{b \in S \mid b \cong a\}$ . Following are logically the same:
- $a \cong b$
  - $a \in [b]$
  - $[a] = [b]$ , the same set
7. Clock arithmetic  $\mathbb{Z}_n$
- (a) Modular equivalence:  $a \equiv b \pmod{n}$  means  $n | a - b$ . Class  $\bar{a} = [a]$ .
- (b) Equivalence class  $\bar{a} = [a]$ .  $\mathbb{Z}_n = \{\bar{0}, \bar{1}, \bar{2}, \dots, \overline{n-1}\}$
- (c) Modular addition and multiplication satisfy all usual rules of algebra
- (d) Modular division:  $\bar{a}^{-1} = \bar{b}$ , where  $\bar{a}\bar{b} = \bar{1}$ , provided  $\gcd(a, n) = 1$ .
- (e) In  $\mathbb{Z}_p$  with  $p$  prime, every  $\bar{a} \neq \bar{0}$  has  $\bar{a}^{-1} \in \mathbb{Z}_p$ .
8. Limits
- (a) Real number axioms: commutative group axioms for  $+$ ,  $\cdot$ ; distributive law' axioms of order  $<$ .
- (b) Completeness: If  $S \subset \mathbb{R}$  has upper bound, then  $\text{lub}(S) = \text{sup}(S) \in \mathbb{R}$ .
- (c) Convergent sequence  $\lim_{n \rightarrow \infty} a_n = \ell$ :  $\forall \epsilon > 0, \exists N, n \geq N \implies |a_n - \ell| < \epsilon$
- (d) Divergent sequence  $(a_n)$ :  $\forall \ell, \exists \epsilon > 0, \forall N, \exists n \geq N$  with  $|a_n - \ell| \geq \epsilon$ .
- (e) Infinite limit  $\lim_{n \rightarrow \infty} a_n = \infty$ :  $\forall B, \exists N, n \geq N \implies a_n > B$ .
- (f) Thm: If  $(a_n)$  increasing bounded sequence, then  $(a_n)$  convergent.

1. Decide whether the following statements are true or false. Prove the true ones and provide counterexamples for the false ones.
  - (a) If  $a_n$  converges, then  $a_n/n$  converges.
  - (b) If  $a_n$  converges and  $b_n$  is bounded, then  $a_n b_n$  converges.
  - (c) If  $a_n \rightarrow \infty$  and  $b_n \rightarrow -\infty$  as  $n \rightarrow \infty$ , then  $a_n + b_n \rightarrow 0$  as  $n \rightarrow \infty$ .
  - (d) If  $a_n \rightarrow 0$  and  $b_n \rightarrow 1$  as  $n \rightarrow \infty$ , then  $b_n/a_n \rightarrow \infty$  as  $n \rightarrow \infty$ .
2. Suppose that  $\{a_n\}$  is bounded. Prove that  $a_n/n^k \rightarrow 0$ , as  $n \rightarrow \infty$  for all  $k \in \mathbb{N}$ .
3. Using the formal definition of the limit prove that if  $\lim_{n \rightarrow \infty} a_n = 1$  then  $\lim_{n \rightarrow \infty} \frac{a_n^2 - e}{a_n} = 1 - e$ .
4. (AC) Let  $S$  be the set of all functions  $f : \mathbb{N} \rightarrow \mathbb{N}$ . Define a relation on  $S$  by letting  $f \sim g$  if and only if  $f(n) = g(n)$  for infinitely many  $n$ . Is this an equivalence relation? If so describe the equivalence classes.
5. (AC) Prove (assuming basic results of calculus) that  $\int_0^\infty x^n e^{-x} dx = n!$ .
6. (AC) For a function  $f : \mathbb{R} \rightarrow \mathbb{R}$ , define  $\lim_{x \rightarrow c} f(x) = L$  to mean that  $\forall \epsilon > 0 \exists \delta > 0$  such that  $\forall x \in \mathbb{R}, |x - c| < \delta \Rightarrow |f(x) - L| < \epsilon$ . Define the function  $f : \mathbb{R} \rightarrow \mathbb{R}$  by

$$s(x) = \begin{cases} 0 & : x \leq 0 \\ 1 & : x > 0 \end{cases}$$

Prove by negating the definition of limit that it is not true that  $\lim_{x \rightarrow 0} s(x) = 0$ .

7. (a) Use a multiplication table to find all values  $a \in \mathbb{Z}_7$  for which the equation

$$x^2 = a$$

has a solution  $x \in \mathbb{Z}_7$ . For each such  $a$ , list all of the solutions  $x$ .

- (b) Find all solutions  $x \in \mathbf{Z}_7$  to the equation  $x^2 + \bar{2}x + \bar{6} = \bar{0}$ .
8. Use quantifiers to express what it means for a sequence  $(x_n)_{n \in \mathbb{N}}$  to *diverge*. You cannot use the terms *not* or *converge*.
9. Suppose  $A, B \subseteq \mathbb{R}$  are bounded and non-empty. Show that  $\sup(A \cup B) = \max\{\sup(A), \sup(B)\}$ .
10. Suppose  $S \subseteq \mathbb{R}$  is bounded and non-empty. Define a new set  $3S$  by  $3S = \{3x \mid x \in S\}$ . Show that  $\sup(3S) = 3\sup(S)$ .
11. Let  $A, B$  be sets, and suppose there is a surjection  $f : A \rightarrow B$ . Prove that there is an injection  $g : B \rightarrow A$ .

12. (a) Define  $x \in \mathbb{R}$  to be a **linear algebraic number** if there are integers  $a, b \in \mathbb{Z}$ , with  $a \neq 0$ , such that  $ax + b = 0$ .  
Prove that the set of linear algebraic numbers is countable. *Hint: Construct an injection into the set  $\mathbb{Z}^2$ .*
- (b) Define  $x \in \mathbb{R}$  to be a **quadratic algebraic number** if there are integers  $a, b, c \in \mathbb{Z}$ , with  $a \neq 0$ , such that  $ax^2 + bx + c = 0$ . Prove that the set of quadratic algebraic numbers is countable. *Hint: Construct an injection into the set  $\mathbb{Z}^3$ .*
13. Use the formal definition of limit to prove the following.
- (a)  $\lim_{n \rightarrow \infty} \frac{n^2 + 3}{2n^3 - 4} = 0$
- (b)  $\lim_{n \rightarrow \infty} \frac{4n - 5}{2n + 7} = 2$
- (c)  $\lim_{n \rightarrow \infty} \frac{n^3 - 3n}{n + 5} = +\infty$
- (d)  $\lim_{n \rightarrow \infty} \frac{n^2 - 7}{1 - n} = -\infty$
14. For each of the following, determine if  $\sim$  defines an equivalence relation on the set  $S$ . If it does, prove it and describe the equivalence classes. If it does not, explain why.
- (a)  $S = \mathbb{R} \times \mathbb{R}$ . For  $(a, b)$  and  $(c, d) \in S$ , define  $(a, b) \sim (c, d)$  if  $3a + 5b = 3c + 5d$ .
- (b)  $S = \mathbb{R}$ . For  $a, b \in S$ ,  $a \sim b$  if  $a < b$ .
- (c)  $S = \mathbb{Z}$ . For  $a, b \in S$ ,  $a \sim b$  if  $a \mid b$ .
- (d)  $S = \mathbb{R} \times \mathbb{R}$ . For  $(a, b)$  and  $(c, d) \in S$ , define  $(a, b) \sim (c, d)$  if  $\lceil a \rceil = \lceil c \rceil$  and  $\lceil b \rceil = \lceil d \rceil$ . Here  $\lceil x \rceil$  is the smallest integer greater than or equal to  $x$ .
15. Consider  $Z_n$ .
- (a) Under what conditions on  $n$  does every nonzero element have a multiplicative inverse? How about an additive inverse?
- (b) Does every nonzero element have a multiplicative inverse in  $Z_{21}$ ?
- (c) Does 5 have a multiplicative inverse in  $Z_{21}$ ? Explain why or why not. If it does, find  $5^{-1}$ .
- (d) Solve the equation  $5x - 14 = 19$  in  $Z_{21}$ .
16. Let  $A = \{a, b, c\}$  and  $B = \{a, x\}$ . List all elements of
- (a)  $A \cup B$
- (b)  $A \cap B$
- (c)  $A \setminus B$

(d)  $A \times B$

(e) Power set of  $A$

17. Let  $S(n) = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid \max\{x, y\} = n\}$ . Prove that  $S(3) \cap S(5)$  is the empty set.

18. Let  $A$  and  $B$  be sets with  $n$  elements. Show that any injective function from  $A$  to  $B$  is surjective as well using induction on  $n$ .

19. Let  $f : \mathbb{N} \rightarrow \mathbb{N}$ , given by  $f(n) = |n - 4|$ .

(a) Prove that  $f$  is surjective

(b) Prove that  $f$  is not injective

20. Let  $f : A \rightarrow B$  and  $g : B \rightarrow A$  be functions satisfying  $f(g(x)) = x$  for all  $x \in B$ . Prove that  $f$  is surjective.

21. Let  $X$  be a set with  $n$  elements and  $B = \{p, q\}$ . Find the number of surjective functions from  $X$  to  $B$ .

22. Describe a concrete bijection from  $\mathbb{N}$  to  $\mathbb{N} \times \{1, 2, 3\}$ . Briefly tell why it is injective and surjective.

23. Make a truth table for  $\text{not } (A \vee B) \implies A \wedge B$ . Find a shorter logically equivalent expression.

24. Find the negations of the following statements:

(a)  $(A \vee B) \wedge (B \vee C)$

(b)  $A \implies (B \wedge C)$

(c)  $\forall x \exists y (P(x) \vee (\text{not } Q(y)))$

1. Decide whether the following statements are true or false. Prove the true ones and provide counterexamples for the false ones.

(a) If  $a_n$  converges, then  $a_n/n$  converges.

**Solution.** This seems reasonable so we will try to prove that it is true. In fact it would make sense that if  $a_n$  converges then  $a_n/n$  should converge to 0. So this is what we will try to show.

**Goal:** to find good  $N_\epsilon$  so that:

$$n \geq N_\epsilon \implies \left| \frac{a_n}{n} - 0 \right| < \epsilon$$

So now please consider:

$$\begin{aligned} \left| \frac{a_n}{n} - 0 \right| &= \left| \frac{a_n - a}{n} + \frac{a}{n} \right| && \text{(Clever splitting of 0)} \\ &\leq \left| \frac{a_n - a}{n} \right| + \left| \frac{a}{n} \right| && \text{(Triangle Ineq.)} \\ &= |a_n - a| \frac{1}{n} + |a| \frac{1}{n} && \text{(n is +)} \end{aligned}$$

Here is where we need to make our good choice for  $N_\epsilon$ . Let's choose  $N_\epsilon = \max\{2, N'_\epsilon, N''_\epsilon\}$  where:

By the definition of  $a_n$  converging we can choose  $N'_\epsilon$  so that :

$$n \geq N'_\epsilon \implies |a_n - a| < \epsilon$$

By since  $\frac{1}{n} \rightarrow 0$  we can choose  $N''_\epsilon$  so that :

$$n \geq N''_\epsilon \implies \left| \frac{1}{n} - 0 \right| = \frac{1}{n} < \frac{\epsilon}{2|a|}$$

And therefore we get if  $n \geq N_\epsilon$  then:

$$\begin{aligned} \left| \frac{a_n}{n} - 0 \right| &\leq |a_n - a| \frac{1}{n} + |a| \frac{1}{n} && \text{(From before)} \\ &< (\epsilon) \frac{1}{2} + |a| \left( \frac{\epsilon}{2|a|} \right) && \text{(Substitutions)} \\ &= \frac{\epsilon}{2} + \frac{\epsilon}{2} && \text{(Simplify)} \end{aligned}$$

And so,

$$\left| \frac{a_n}{n} - 0 \right| < \epsilon$$

So therefore by the definition of convergence  $\frac{a_n}{n}$  **converges** (to 0). And so this statement is **TRUE**.

Lastly I should note that the choosing of  $N_\epsilon$  takes some time and lots of scrap paper to work out. There is an easier way! If you use the theorem that says **Every convergent sequence is bounded** it is very straightforward. Try it out (Or look at the proof of 2)!

(b) If  $a_n$  converges and  $b_n$  is bounded, then  $a_n b_n$  converges.

**Solution.** Let's review with the definition of bounded:

**Definition:**

$$\{x_n\} \text{ is bounded} \Leftrightarrow \exists M > 0 \text{ such that } x_n \leq M \forall n \in \mathbb{N}$$

Let's try for a counterexample. Let's take some very simple choices:

$$a_n = 1 = \{1, 1, 1, \dots\}$$

$$b_n = (-1)^n = \{-1, 1, -1, \dots\}$$

Then  $a_n$  obviously converges (to 1) and  $b_n$  is bounded by  $M = 1$ . and yet:

$$a_n b_n = 1(-1)^n = (-1)^n \text{ which does not converge.}$$

And so this statement is **FALSE**.

(c) If  $a_n \rightarrow \infty$  and  $b_n \rightarrow -\infty$  as  $n \rightarrow \infty$ , then  $a_n + b_n \rightarrow 0$  as  $n \rightarrow \infty$ .

**Solution.** This should not be true. because things can head to  $\pm\infty$  at different rates. Let's try for a counter-example. Let's choose:

$$a_n = 2n$$

$$b_n = -n$$

Then we can see that these meet the criteria of  $a_n \rightarrow \infty$  and  $b_n \rightarrow -\infty$  and yet:

$$a_n + b_n = 2n + (-n) = n \rightarrow \infty \neq 0$$

And so this statement is **FALSE**.

(d) If  $a_n \rightarrow 0$  and  $b_n \rightarrow 1$  as  $n \rightarrow \infty$ , then  $b_n/a_n \rightarrow \infty$  as  $n \rightarrow \infty$ .

**Solution.** The claim is that this is FALSE and this will be because we could have  $a_n \rightarrow 0$  and yet  $a_n < 0 \forall n$  which would yield  $b_n/a_n \rightarrow -\infty$ .

So let's take

$$b_n = 1 \rightarrow 1$$

$$a_n = -\frac{1}{n} \rightarrow 0$$

Then we can look at:

$$b_n/a_n = 1 / \left( -\frac{1}{n} \right) = \boxed{-n \rightarrow -\infty \neq \infty}$$

And so this statement is **FALSE**.

Let's quickly take some practice formally showing that  $-n \rightarrow -\infty$ . Let's first recall a definition of what we mean by a sequence  $x_n \rightarrow \pm\infty$ .

**Definition:**  $x_n \rightarrow \infty$  means:

$$\forall M \in \mathbb{R}, \exists N_M \in \mathbb{N} \text{ such that: } n \geq N_M \implies x_n > M.$$

**Definition:**  $x_n \rightarrow -\infty$  means:

$$\forall M \in \mathbb{R}, \exists N_M \in \mathbb{N} \text{ such that: } n \geq N_M \implies x_n < M.$$

So it is now clear what we have to do:

**Goal:** to choose a good  $N_M$  so that:

$$n \geq N_M \implies -n < M$$

Since  $M \in \mathbb{R}$  we need to do a little extra work to make sure that we choose  $N_M \in \mathbb{N}$  but still it is not so bad.

Let's try:  $N_M = \lceil |M| \rceil + 1$  (the ceiling function where we just round up of the absolute value.) So now

$$n \geq \lceil |M| \rceil + 1 \implies -n \leq \lceil |M| \rceil - 1 < M$$

And so we have  $\boxed{n \geq N_M \implies -n < M}$  so by the definition:  $\boxed{-n \rightarrow -\infty}$

Honestly though I had to sit and play with this for quite some time to see that  $N_M = \lceil |M| \rceil + 1$  was a good choice. To help me I considered what if  $M = -4.5$  or what if  $M = 4.5$  to help me:

If  $M = -4.5$  then we get

$$N_M = \lceil |-4.5| \rceil + 1 = \lceil 4.5 \rceil + 1 = 5 + 1 = 6 \text{ so we get } n \geq 6 \implies -n < -4.5$$

Or if  $M = 4.5$  then we get

$$N_M = \lceil |4.5| \rceil + 1 = \lceil 4.5 \rceil + 1 = 5 + 1 = 6 \text{ so we get } n \geq 6 \implies -n < 4.5$$

Choosing nice specific examples like this can help craft good choices of  $N_M$  (or  $\delta$  or  $N_\epsilon$ ) on occasion.



2. Suppose that  $\{a_n\}$  is bounded. Prove that  $a_n/n^k \rightarrow 0$ , as  $n \rightarrow \infty$  for all  $k \in \mathbb{N}$ .

**Solution.** The first step is to perform some simplifications. Let's apply the following theorem

**Theorem:**

$$x_n \rightarrow 0 \quad \Leftrightarrow \quad |x_n| \rightarrow 0$$

Which is a result of the Squeeze Theorem. So therefore  $a_n/n^k \rightarrow 0 \Leftrightarrow |a_n|/n^k \rightarrow 0$ .

Now let's apply the Squeeze Theorem directly which states:

**Theorem:** (Squeeze)

If  $x_n \rightarrow a$  and  $y_n \rightarrow a$  and if  $x_n \leq w_n \leq y_n \quad \forall n \geq N_0$  then:

$$w_n \rightarrow a$$

Our desired thing to show converges is  $|a_n|/n^k \rightarrow 0$ . So let's make good choice for  $x_n \rightarrow 0$  and  $y_n \rightarrow 0$  so that the Squeeze Theorem will help us.

Since we have  $0 \leq |a_n|/n^k$  we can take  $x_n = 0 \rightarrow 0$ . Now for  $y_n$  let's use the fact that  $a_n$  bounded, which means that:

$$\exists M > 0 \text{ such that } a_n \leq M \quad \forall n \in \mathbb{N}$$

Also if  $n, k \geq 1$  then  $n \leq n^k \implies \frac{1}{n^k} \leq \frac{1}{n}$ . Combining these we have that  $|a_n|/n^k \leq M/n^k \leq M/n$ .

So therefore we should choose  $y_n = M/n$  which converges to 0 by the multiplicative rule of limits

$$\frac{M}{n} = M \frac{1}{n} \rightarrow M(0) = 0$$

By the Squeeze theorem we win!

3. Using the formal definition of the limit proof that if  $\lim_{n \rightarrow \infty} a_n = 1$  then  $\lim_{n \rightarrow \infty} \frac{a_n^2 - e}{a_n} = 1 - e$ .

**Solution.** This would be much easier if we could use properties of limits. Let's try it out using the definition though:

**Goal:** to find good  $N_\epsilon$  so that:

$$n \geq N_\epsilon \implies \left| \frac{a_n^2 - e}{a_n} - (1 - e) \right| < \epsilon$$

We have in our tool belt that  $a_n \rightarrow 1$  which means:

$$\forall \epsilon' > 0 \exists N'_\epsilon \in \mathbb{N} \text{ so that: } n \geq N'_\epsilon \implies |a_n - 1| < \epsilon' \quad (**)$$

So let's rearrange  $\left| \frac{a_n^2 - e}{a_n} - (1 - e) \right|$  a bit and see if there is any natural progressions!

$$\begin{aligned} \left| \frac{a_n^2 - e}{a_n} - (1 - e) \right| &= \left| \frac{a_n^2 - e - a_n + ea_n}{a_n} \right| && \text{(Common Denominator)} \\ &= \left| \frac{a_n^2 + (e - 1)a_n - e}{a_n} \right| && \text{(Rearrange to look like Quadratic)} \\ &= \left| \frac{(a_n + e)(a_n - 1)}{a_n} \right| && \text{(Factor)} \\ &= \left| \frac{a_n + e}{a_n} \right| |a_n - 1| && \text{(Property of } |\cdot| \text{)} \end{aligned}$$

Here we need to employ some trick to bound  $\left| \frac{a_n + e}{a_n} \right|$ . Let's consider  $N''_\epsilon$  so that

$$n \geq N''_\epsilon \implies |a_n - 1| < .5 \implies .5 < a_n < 1.5.$$

Now to make it look like  $\left| \frac{a_n + e}{a_n} \right|$ .

$$.5 < a_n < 1.5 \implies 0 < .5 + e < a_n + e < 1.5 + e \implies 0 < \frac{a_n + e}{a_n} < \frac{1.5 + e}{.5} = 3 + 2e \implies \boxed{\left| \frac{a_n + e}{a_n} \right| < 3 + 2e}$$

So let's consider choosing  $N'_\epsilon$  from (\*\*) so that:

$$n \geq N'_\epsilon \implies \boxed{|a_n - 1| < \frac{\epsilon}{3 + 2e}}$$

Finally taking  $N_\epsilon = \max\{N'_\epsilon, N''_\epsilon\}$  gives us:

$$n \geq N_\epsilon \implies \left| \frac{a_n + e}{a_n} \right| |a_n - 1| < (3 + 2e) \left( \frac{\epsilon}{3 + 2e} \right) = \epsilon$$

Making us the winners!

4. (AC) Let  $S$  be the set of all functions  $f : \mathbb{N} \rightarrow \mathbb{N}$ . Define a relation on  $S$  by letting  $f \sim g$  if and only if  $f(n) = g(n)$  for infinitely many  $n$ . Is this an equivalence relation? If so describe the equivalence classes.

**Solution.** The relation is reflexive since for any  $f : \mathbb{N} \rightarrow \mathbb{N}$ ,  $f(n) = f(n) \forall n \in \mathbb{N}$  where  $\mathbb{N}$  is an infinite set. The relation is symmetric since  $=$  is symmetric. In fact, the relation is not transitive. To see why, consider the following functions. Let  $f(n)$  be equal to 1 for  $n$  even and 2 for  $n$  odd. Let  $g(n)$  be equal to 3 for  $n$  even and 2 for  $n$  odd. Let  $h(n)$  be equal to 3 for  $n$  even and 4 for  $n$  odd. Then  $f \sim g$  and  $g \sim h$  but  $f$  and  $h$  agree nowhere.

5. (AC) Prove (assuming basic results of calculus) that  $\int_0^\infty x^n e^{-x} dx = n!$ .

**Solution.** We proceed by induction on  $n \geq 0$ . The base case holds since

$$\begin{aligned} \int_0^\infty e^{-x} dx &= \lim_{b \rightarrow \infty} \int_0^b e^{-x} dx \\ &= \lim_{b \rightarrow \infty} -e^{-x} \Big|_0^b \\ &= \lim_{b \rightarrow \infty} -e^{-b} + 1 \\ &= 1 \\ &= 0! \end{aligned}$$

To show that the inductive step holds, we integrate by parts with  $u = x^n$ ,  $dv = e^{-x} dx$ . We have

$$\begin{aligned} \int_0^\infty x^n e^{-x} dx &= \lim_{b \rightarrow \infty} \int_0^b x^n e^{-x} dx \\ &= \lim_{b \rightarrow \infty} \left[ x^n (-e^{-x}) \Big|_0^b - \int_0^b nx^{n-1} [-e^{-x}] dx \right] \\ &= 0 + n \int_0^\infty x^{n-1} e^{-x} dx \\ &= n(n-1)! && \text{by the inductive hypothesis} \\ &= n!. \end{aligned}$$

Thus by induction, the identity holds for all  $n \geq 0$ .

6. (AC) For a function  $f : \mathbb{R} \rightarrow \mathbb{R}$ , define  $\lim_{x \rightarrow c} f(x) = L$  to mean that  $\forall \epsilon > 0 \exists \delta > 0$  such that  $\forall x \in \mathbb{R}, |x - c| < \delta \Rightarrow |f(x) - L| < \epsilon$ . Define the function  $f : \mathbb{R} \rightarrow \mathbb{R}$  by

$$s(x) = \begin{cases} 0 & : x \leq 0 \\ 1 & : x > 0 \end{cases}$$

Prove by negating the definition of limit that it is not true that  $\lim_{x \rightarrow 0} s(x) = 0$ .

**Solution.** The negation of  $\lim_{x \rightarrow 0} s(x) = 0$  is

$$\exists \epsilon > 0 \text{ such that } \forall \delta > 0, \exists x \in \mathbb{R} \text{ such that } |x - 0| < \delta \text{ and } |s(x) - 0| \geq \epsilon$$

Letting  $\epsilon = 1/2$ , then  $\forall \delta > 0, \delta/2 \in \mathbb{R}$  with  $|\delta/2 - 0| = \delta/2 < \delta$  and  $|s(\delta/2) - 0| = |1 - 0| = 1 \geq 1/2$ . Thus the limit is not equal to 0.

7. (a) Use a multiplication table to find all values  $a \in \mathbb{Z}_7$  for which the equation

$$x^2 = a$$

has a solution  $x \in \mathbb{Z}_7$ . For each such  $a$ , list all of the solutions  $x$ .

**Solution.** We only need to look at the diagonal of the multiplication table for  $\mathbb{Z}_7$ . Then the equation  $x^2 = a$  has a solution  $x \in \mathbb{Z}_7$  if and only if  $a \in \{\bar{0}, \bar{1}, \bar{2}, \bar{4}\}$ . When  $a = \bar{0}$ , the only solution is  $x = \bar{0}$ . When  $a = \bar{1}$ , the solutions are  $x = \bar{1}$  and  $x = \bar{6}$ . When  $a = \bar{2}$ , the solutions are  $x = \bar{3}$  and  $x = \bar{4}$ . When  $a = \bar{4}$ , the solutions are  $x = \bar{2}$  and  $x = \bar{5}$ .

- (b) Find all solutions  $x \in \mathbb{Z}_7$  to the equation  $x^2 + \bar{2}x + \bar{6} = \bar{0}$ .

**Solution.** Adding  $\bar{2}$  to both sides, the given equation is equivalent to  $x^2 + \bar{2}x + \bar{1} = \bar{2}$ . We can factor the left-hand side to get

$$(x + \bar{1})^2 = \bar{2}.$$

It follows from part (a) that  $x + \bar{1} = \bar{3}$  or  $x + \bar{1} = \bar{4}$ , and hence  $x = \bar{2}$  or  $x = \bar{3}$ .

8. Use quantifiers to express what it means for a sequence  $(x_n)_{n \in \mathbb{N}}$  to *diverge*. You cannot use the terms *not* or *converge*.

**Solution.** A sequence  $(x_n)_{n \in \mathbb{N}}$  *diverges* if for every  $L \in \mathbb{R}$  there is some  $\epsilon > 0$  such that for all  $N \in \mathbb{N}$  there is some natural number  $n \geq N$  for which  $|x_n - L| \geq \epsilon$ . In terms of quantifiers this is

$$\forall L \in \mathbb{R} \exists \epsilon > 0 \forall N \in \mathbb{N} \exists n \geq N, |x_n - L| \geq \epsilon.$$

9. Suppose  $A, B \subseteq \mathbb{R}$  are bounded and non-empty. Show that  $\sup(A \cup B) = \max\{\sup(A), \sup(B)\}$ .

**Solution.** First note that since  $A$  and  $B$  are both bounded and non-empty, the same is true of  $A \cup B$  and so  $\sup(A \cup B) \in \mathbb{R}$  exists. It follows immediately from Beck Proposition 8.50 that  $\sup(A \cup B) \geq \max\{\sup(A), \sup(B)\}$ , since  $A$  and  $B$  are both subsets of  $A \cup B$ . We need to prove the reverse inequality. For sake of contradiction, suppose  $\sup(A \cup B) > \max\{\sup(A), \sup(B)\}$ . Then neither  $\sup(A)$ , nor  $\sup(B)$  can be an upper bound for  $A \cup B$ . So there is some  $x \in A \cup B$  with  $x > \sup(A)$  and  $x > \sup(B)$ . But  $x \in A \cup B$  implies that  $x \in A$  or  $x \in B$ , so this cannot happen.

10. Suppose  $S \subseteq \mathbb{R}$  is bounded and non-empty. Define a new set  $3S$  by  $3S = \{3x \mid x \in S\}$ . Show that  $\sup(3S) = 3\sup(S)$ .

**Solution.** First we will show  $\sup(3S) \leq 3\sup(S)$ . Let  $y \in 3S$ . Then  $y = 3x$  for some  $x \in S$ . Since  $\sup(S)$  is an upper bound for  $S$ , we have  $x \leq \sup(S)$ . This gives  $y = 3x \leq 3\sup(S)$ . Since this is true for all  $y \in 3S$ , it follows that  $3\sup(S)$  is an upper bound for the set  $3S$ . Since  $\sup(3S)$  is the *least* upper bound, we must have  $\sup(3S) \leq 3\sup(S)$ .

To prove the reverse inequality, let  $x \in S$ . Then  $3x \in 3S$  and so  $3x \leq \sup(3S)$ . Equivalently,  $x \leq 3^{-1}\sup(3S)$ . It follows that  $3^{-1}\sup(3S)$  is an upper bound for  $S$  and so  $\sup(S) \leq 3^{-1}\sup(3S)$ , since  $\sup(S)$  is the *least* upper bound.

Multiplying both sides by 3 proves the result.

11. Let  $A, B$  be finite sets, and suppose there is a surjection  $f : A \rightarrow B$ . Prove that there is an injection  $g : B \rightarrow A$  such that  $f \circ g : B \rightarrow B$  is the identity function.

**Solution.** Let  $b \in B$ , we want to define  $g(b) \in A$ . Since  $f$  is surjective, it follows that  $f^{-1}(b)$  is a non-empty set. Let  $a \in f^{-1}(b)$  be any element of this set, and declare  $g(b) = a$ . We obviously have that  $f \circ g$  is the identity, since  $f(g(b)) = f(a) = b$  for all  $b \in B$ . To show  $g$  is injective, suppose there are  $b, b' \in B$  with  $g(b) = g(b')$ . Let  $a = g(b)$  denote this common value. Then by construction of  $g$ , we have  $a \in f^{-1}(b)$  and  $a \in f^{-1}(b')$ . Applying  $f$  to  $a$  therefore gives  $f(a) = b$  and  $f(a) = b'$ , and so  $b = b'$ .

12. (a) Define  $x \in \mathbb{R}$  to be a **linear algebraic number** if there are integers  $a, b \in \mathbb{Z}$ , with  $a \neq 0$ , such that  $ax + b = 0$ . Prove that the set of linear algebraic numbers is countable. *Hint: Construct an injection into the set  $\mathbb{Z}^2$ .*

**Solution.** Since  $\mathbb{Z}^2$  is countable, it suffices to show that there is an injection from the set of linear algebraic numbers into  $\mathbb{Z}^2$ . Given a linear algebraic number  $x$ , there are  $a, b \in \mathbb{Z}$  with  $ax + b = 0$ , and  $a \neq 0$ . (Note that there will be multiple choices of  $a, b$  for which  $ax + b = 0$ . However, we can choose  $a, b$  canonically by requiring  $a > 0$  and  $\gcd(a, b) = 1$ .) Then we define the function by sending  $x$  to these values of  $a, b$ . To see that this function is injective, suppose there are  $a, b \in \mathbb{Z}$  with  $a \neq 0$  and  $ax + b = ay + b$  for some  $x, y \in \mathbb{R}$ . Then obviously  $x = y$ , since  $a \neq 0$ . (Note that the linear algebraic numbers are exactly the rational numbers, and we are just proving that  $\mathbb{Q}$  is countable.)

- (b) Define  $x \in \mathbb{R}$  to be a **quadratic algebraic number** if there are integers  $a, b, c \in \mathbb{Z}$ , with  $a \neq 0$ , such that  $ax^2 + bx + c = 0$ . Prove that the set of quadratic algebraic numbers is countable. *Hint: Construct an injection into the set  $\mathbb{Z}^3$ .*

**Solution.** We will show that there is an injective function from the set of quadratic algebraic numbers into  $\mathbb{Z}^3$ . Given a quadratic algebraic number  $x$ , there are  $a, b, c \in \mathbb{Z}$  with  $ax^2 + bx + c = 0$ , and  $a \neq 0$ . As in part (a), the basic idea is to send  $x$  to  $(a, b, c) \in \mathbb{Z}^3$ . However, there is an extra feature of this problem that makes it a little more difficult, and this is coming from the fact that most quadratic equations have 2 solutions (this will mean that our function will not be injective, unless we are careful). Here is a way to define the function so that it is injective. Let  $x$  be as above. If there is some  $x' \in \mathbb{R}$  with  $a(x')^2 + bx' + c = 0$  and  $x \neq x'$ , then without loss of generality we may suppose  $x' < x$ . Send  $x$  to  $(a, b, c)$  where  $a > 0$  and  $a, b, c$  have no common divisors, and send  $x'$  to  $(-a, -b, -c)$ . (Note that by the quadratic formula there can be at most two solutions of  $ax^2 + bx + c = 0$ .) To see that this function is injective, suppose  $x_1$  and  $x_2$  are both sent to  $(a, b, c)$ . This implies that  $x_1, x_2$  are both solutions to the equation  $ax^2 + bx + c = 0$ . If  $a > 0$ , then by construction of our function,  $x_1$  and  $x_2$  are both equal to the solution with the maximum values and so  $x_1 = x_2$ . If  $a < 0$ , then  $x_1$  and  $x_2$  are both equal to the solution with the smallest value and so  $x_1 = x_2$ .

13. Use the formal definition of limit to prove the following.

(a)  $\lim_{n \rightarrow \infty} \frac{n^2 + 3}{2n^3 - 4} = 0$

**Solution.** Let  $\varepsilon > 0$  be given, arbitrary. Define  $N = \max\{3, \frac{2}{\varepsilon} + 2\}$ . Let  $n \geq N$ ,  $n \in \mathbb{N}$  be arbitrary. Then,

$$\begin{aligned} \left| \frac{n^2 + 3}{2n^3 - 4} - 0 \right| &= \frac{n^2 + 3}{2n^3 - 4} && \text{(since } n \geq 3) \\ &\leq \frac{n^2 + 3n^2}{2n^3 - 4n^2} && \text{(We increased the numerator and decreased the denominator,} \\ &&& \text{keeping in mind } 2n^3 - 2n^2 > 0, \text{ as } n > 2) \\ &= \frac{2}{n - 2} && \text{(Factor and cancel out common terms)} \\ &\leq \frac{2}{N - 2} && (n \geq N) \\ &\leq \varepsilon && (N \geq \frac{2}{\varepsilon} + 2) \end{aligned}$$

Thus,  $\forall \varepsilon > 0$ ,  $\exists N$  such that  $\forall n > N$  with  $n \in \mathbb{N}$ ,  $\left| \frac{n^2 + 3}{2n^3 - 4} - 0 \right| < \varepsilon$ . Thus, indeed  $\lim_{n \rightarrow \infty} \frac{n^2 + 3}{2n^3 - 4} = 0$ .

(b)  $\lim_{n \rightarrow \infty} \frac{4n - 5}{2n + 7} = 2$

**Solution.** Let  $\varepsilon > 0$  be given, arbitrary. Define  $N = \frac{1}{\varepsilon}$ . Let  $n \geq N$ ,  $n \in \mathbb{N}$  be arbitrary. Then,

$$\begin{aligned} \left| \frac{4n - 5}{2n + 7} - 2 \right| &= \frac{19}{2n + 7} && \text{(since } n > 0) \\ &< \frac{19}{2n} && \text{(We decreased the denominator,} \\ &< \frac{1}{n} && \\ &\leq \frac{1}{N} && (n \geq N) \\ &= \varepsilon && (N = \frac{1}{\varepsilon}) \end{aligned}$$

Thus,  $\forall \varepsilon > 0$ ,  $\exists N$  such that  $\forall n > N$  with  $n \in \mathbb{N}$ ,  $\left| \frac{4n - 5}{2n + 7} - 2 \right| < \varepsilon$ . Thus, indeed  $\lim_{n \rightarrow \infty} \frac{4n - 5}{2n + 7} = 2$ .

(c)  $\lim_{n \rightarrow \infty} \frac{n^3 - 3n}{n + 5} = +\infty$

**Solution.** Let  $M > 0$  be given, arbitrary. Define  $N = \sqrt{6M + 3}$ . Let  $n \geq N$ ,  $n \in \mathbb{N}$  be arbitrary. Then,

$$\begin{aligned} \frac{n^3 - 3n}{n + 5} &\geq \frac{n^3 - 3n}{n + 5n} && (\text{since } n \geq 1) \\ &= \frac{n^3 - 3n}{6n} \\ &= \frac{n^2 - 3}{6} \\ &\geq \frac{N^2 - 3}{6} && (n \geq N) \\ &= M && (N = \sqrt{6M + 3}) \end{aligned}$$

Thus,  $\forall M > 0$ ,  $\exists N$  such that  $\forall n > N$  with  $n \in \mathbb{N}$ ,  $\frac{n^3 - 3n}{n + 5} \geq M$ . Thus, indeed  $\lim_{n \rightarrow \infty} \frac{n^3 - 3n}{n + 5} = +\infty$ .

(d)  $\lim_{n \rightarrow \infty} \frac{n^2 - 7}{1 - n} = -\infty$

**Solution.** Let  $M < 0$  be given, arbitrary. Define  $N = 7 - M$ . Let  $n \geq N$ ,  $n \in \mathbb{N}$  be arbitrary. Then,

$$\begin{aligned} \frac{n^2 - 7}{1 - n} &< \frac{n^2 - 7}{-n} && (\text{since } n > 7, \text{ thus } n^2 - 7 > 0) \\ &\leq \frac{n^2 - 7n}{-n} && (\text{since the denominator is negative and } n > 7, \\ &&& \text{decreasing the numerator, while still keeping it positive}) \\ &= 7 - n \\ &\leq 7 - N && (n \geq N) \\ &= M && (N = 7 - M) \end{aligned}$$

Thus,  $\forall M < 0$ ,  $\exists N$  such that  $\forall n > N$  with  $n \in \mathbb{N}$ ,  $\frac{n^2 - 7}{1 - n} \leq M$ . Thus, indeed  $\lim_{n \rightarrow \infty} \frac{n^2 - 7}{1 - n} = -\infty$ .

14. For each of the following, determine if  $\sim$  defines an equivalence relation on the set  $S$ . If it does, prove it and describe the equivalence classes. If it does not, explain why.

(a)  $S = \mathbb{R} \times \mathbb{R}$ . For  $(a, b)$  and  $(c, d) \in S$ , define  $(a, b) \sim (c, d)$  if  $3a + 5b = 3c + 5d$ .



**Solution.** The relation  $\sim$  as defined above is indeed an equivalence relation, since it satisfies reflexivity, symmetry and transitivity, as shown below.

- Reflexivity: Let  $(a, b) \in S$ . Then  $3a + 5b = 3a + 5b$ , and therefore  $(a, b) \sim (a, b)$ .
- Symmetry: Let  $(a, b), (c, d) \in S$  such that  $(a, b) \sim (c, d)$ . Then  $3a + 5b = 3c + 5d$ . This is equivalent to  $3c + 5d = 3a + 5b$ , which implies  $(c, d) \sim (a, b)$ .
- Transitivity: Let  $(a, b), (c, d), (e, f) \in S$ , such that  $(a, b) \sim (c, d)$  and  $(c, d) \sim (e, f)$ . Then  $3a + 5b = 3c + 5d$  and  $3c + 5d = 3e + 5f$ . By transitivity of equality for real numbers we have  $3a + 5b = 3e + 5f$ , and therefore  $(a, b) \sim (e, f)$ .

The equivalence classes are the lines  $3x + 5y = c$ , i.e. each equivalence class is a line with slope  $-\frac{3}{5}$  and the different equivalence classes have different  $y$ -intercepts (given by  $\frac{c}{5}$ ).

(b)  $S = \mathbb{R}$ . For  $a, b \in S$ ,  $a \sim b$  if  $a < b$ .

**Solution.** The relation defined by  $a \sim b$  if  $a < b$  is not an equivalence relation, since it does not satisfy reflexivity. Namely,  $a \not\sim a$ , since  $a \not< a$ .

(c)  $S = \mathbb{Z}$ . For  $a, b \in S$ ,  $a \sim b$  if  $a \mid b$ .

**Solution.** The relation defined by  $a \sim b$  if  $a \mid b$  is not an equivalence relation, since it does not satisfy symmetry. Namely,  $a \sim b$  does not necessarily imply  $b \sim a$ . For example,  $2 \mid 8$ , but  $8 \nmid 2$ .

(d)  $S = \mathbb{R} \times \mathbb{R}$ . For  $(a, b)$  and  $(c, d) \in S$ , define  $(a, b) \sim (c, d)$  if  $\lceil a \rceil = \lceil c \rceil$  and  $\lceil b \rceil = \lceil d \rceil$ . Here  $\lceil x \rceil$  is the smallest integer greater than or equal to  $x$ .

**Solution.** The relation  $\sim$  as defined above is indeed an equivalence relation, since it satisfies reflexivity, symmetry and transitivity, as shown below.

- Reflexivity: Let  $(a, b) \in S$ . Then  $\lceil a \rceil = \lceil a \rceil$  and  $\lceil b \rceil = \lceil b \rceil$ , and therefore  $(a, b) \sim (a, b)$ .
- Symmetry: Let  $(a, b), (c, d) \in S$  such that  $(a, b) \sim (c, d)$ . Then  $\lceil a \rceil = \lceil c \rceil$  and  $\lceil b \rceil = \lceil d \rceil$ . This is equivalent to  $\lceil c \rceil = \lceil a \rceil$  and  $\lceil d \rceil = \lceil b \rceil$ , which implies  $(c, d) \sim (a, b)$ .
- Transitivity: Let  $(a, b), (c, d), (e, f) \in S$ , such that  $(a, b) \sim (c, d)$  and  $(c, d) \sim (e, f)$ . Then  $\lceil a \rceil = \lceil c \rceil$  and  $\lceil b \rceil = \lceil d \rceil$ , as well as  $\lceil c \rceil = \lceil e \rceil$  and  $\lceil d \rceil = \lceil f \rceil$ . By transitivity of equality for real numbers we have  $\lceil a \rceil = \lceil e \rceil$  and  $\lceil b \rceil = \lceil f \rceil$ , and therefore  $(a, b) \sim (e, f)$ .

The equivalence classes are squares in the plane  $\mathbb{R}^2$  with sides parallel to the coordinate axes, in particular, they are sets of the form  $(i, i + 1] \times (j, j + 1]$  (Cartesian product of intervals), where the ordered pair  $(i, j) \in \mathbb{Z}^2$ .

15. Consider  $Z_n$ .

- (a) Under what conditions on  $n$  does every nonzero element have a multiplicative inverse? How about an additive inverse?

**Solution.** Every nonzero element in  $Z_n$  has a multiplicative inverse if  $n$  is prime. Indeed, if  $n$  is prime,  $\gcd(n, m) = 1 \forall m \in \mathbb{Z}$  such that  $0 < m < n$ , and therefore by Bezout's Lemma there exist integers  $x, y$  such that  $nx + my = 1$ , thus  $my \equiv 1 \pmod{n}$ , i.e.  $\bar{m} \cdot \bar{y} = 1$ , which implies that  $\bar{m}^{-1} = \bar{y}$ .

Every element in  $Z_n$  does have an additive inverse  $\forall n \in \mathbb{N}$ .

- (b) Does every nonzero element have a multiplicative inverse in  $Z_{21}$ ?

**Solution.** No, one can check that  $\bar{3}$  and  $\bar{7}$  do not have multiplicative inverses in  $Z_{21}$ .

- (c) Does 5 have a multiplicative inverse in  $Z_{21}$ ? Explain why or why not. If it does, find  $5^{-1}$ .

**Solution.** One can express  $\gcd(5, 21)$  in the form  $5x + 21y$  for some integers  $x, y$  by applying the Euclidean Algorithm,  $21 = 4 \cdot 5 + 1$ , therefore  $5 \cdot (-4) + 21 \cdot 1 = 1$ , thus  $\bar{5}^{-1} = \bar{17}$ . (Note that the equivalence classes  $\bar{-4} = \bar{17}$ .)

- (d) Solve the equation  $5x - 14 = 19$  in  $Z_{21}$ .

**Solution.** The equation  $\bar{5}x - \bar{14} = \bar{19}$  is equivalent to  $\bar{5}x = \bar{12}$ , which, using that  $\bar{5}^{-1} = \bar{17}$  yields  $x = \bar{12} \cdot \bar{17} = \bar{15}$ .

16. Let  $A = \{a, b, c\}$  and  $B = \{a, x\}$ . List all elements of

- (a)  $A \cup B$
- (b)  $A \cap B$
- (c)  $A \setminus B$
- (d)  $A \times B$
- (e) Power set of  $A$

**Solution.**  $A \cup B = \{a, b, c, x\}$ ,  $A \cap B = \{a\}$ ,  $A \setminus B = \{b, c\}$ ,  $A \times B = \{(a, a), (a, x), (b, a), (b, x), (c, a), (c, x)\}$ ,

Power set of  $A$  is  $\{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{b, c\}, \{a, c\}, \{a, b, c\}\}$ .

17. Let  $S(n) = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid \max\{x, y\} = n\}$ . Prove that  $S(3) \cap S(5)$  is the empty set.

**Solution.** Assume the contrary: let  $(a, b) \in S(3) \cap S(5)$ . Then  $\max\{a, b\} = 3$  and  $\max\{a, b\} = 5$ , but  $3 \neq 5$ , hence our assumption leads to a contradiction. Therefore the intersection is empty.

18. Let  $A$  and  $B$  be sets with  $n$  elements. Show that any injective function from  $A$  to  $B$  is surjective as well using induction on  $n$ .

**Solution.** *Base case,  $n = 1$ .* Since  $A = \{a_1\}$  and  $B = \{b_1\}$  have only one element each, there is only one function  $f$ , given by  $f(a_1) = b_1$  which is injective ( $f(x) = f(y)$  implies  $x = y = a_1$  since  $A$  consists only of  $a_1$ ) and surjective ( $b_1$  is the image of  $a_1$  under  $f$ ).

*Inductive Hypothesis.* Assume  $A$  and  $B$  are sets with  $n = k$  elements and that any injective function from  $A$  to  $B$  is surjective.

*Inductive Step.* Show that the same statement is true for  $n = k + 1$ : Let  $A = \{a_1, \dots, a_{k+1}\}$  and  $B = \{b_1, \dots, b_{k+1}\}$ . Let  $A' = A \setminus \{a_{k+1}\}$  and  $B' = B \setminus \{b_{k+1}\}$ . Since  $f$  is injective,  $f(A')$  does not contain  $f(a_{k+1})$ , hence  $f$  restricts to a function  $f'$  from  $A'$  to  $B'$ , both of which have  $k$  elements. Claim:  $f'$  is injective (short proof), hence by the inductive hypothesis,  $f'$  is surjective. To check that  $f$  is surjective, if  $b = f(a_{k+1})$ ,  $b$  is the image of  $a_{k+1}$ , otherwise, for any  $b \in B$  with  $b \neq f(a_{k+1})$ , we have  $b \in B'$ , hence  $b = f'(a_i)$  for some  $i$ , hence  $b = f(a_i)$ .

19. Let  $f : \mathbb{N} \rightarrow \mathbb{N}$ , given by  $f(n) = |n - 4|$ .

- (a) Prove that  $f$  is surjective
- (b) Prove that  $f$  is not injective

**Solution.** Given  $y \in \mathbb{N}$ ,  $f(y + 4) = |y + 4 - 4| = y$  since  $y \geq 0$ , which shows that  $f$  is surjective.  $f(1) = 3 = f(7)$ , hence  $f$  is not injective.

20. Let  $f : A \rightarrow B$  and  $g : B \rightarrow A$  be functions satisfying  $f(g(x)) = x$  for all  $x \in B$ . Prove that  $f$  is surjective.

**Solution.** First attempt: Assume  $f$  is not surjective. Then there is a  $b \in B$  such that there are no  $a \in A$  with  $f(a) = b$ . Let  $c = g(b)$ , then  $f(c) = f(g(b)) = b$  by assumption, hence we found a  $c \in A$  with  $f(c) = b$  which contradicts with the assumption.

Second attempt: Given  $b \in B$ , let  $a = g(b)$ , and compute  $f(a) = f(g(b)) = b$  by assumption. Since  $b$  was arbitrary, this shows that  $f$  is surjective.

21. Let  $X$  be a set with  $n$  elements and  $B = \{p, q\}$ . Find the number of surjective functions from  $X$  to  $B$ .

**Solution.** There are  $2 \cdot 2 \cdot \dots \cdot 2 = 2^n$  possible functions from  $X$  to  $B$ . Now list all functions that are not surjective (there are exactly two, tell which ones), hence we get  $2^n - 2$ .

22. Describe a concrete bijection from  $\mathbb{N}$  to  $\mathbb{N} \times \{1, 2, 3\}$ . Briefly tell why it is injective and surjective.

**Solution.** By division lemma, given  $n$ , there is a unique  $q$  and  $r$  with  $0 \leq r < 3$  with  $n = 3 \cdot q + r$ , we could define  $f(n)$  by  $f(n) = (q, r + 1)$ . Then  $f$  has the inverse function given by  $g(a, b) = 3 \cdot a + b$ . Check that  $f(g(a, b)) = (a, b)$  and  $g(f(n)) = n$ .

23. Make a truth table for  $\text{not}(A \vee B) \implies A \wedge B$ . Find a shorter logically equivalent expression.

**Solution.** Consider all possibilities for simultaneous truth values for  $A$  and  $B$ :

$A$	$B$	$\text{not}(A \vee B)$	$A \wedge B$	$\text{not}(A \vee B) \implies \text{not} A$
T	T	F	T	T
T	F	F	F	T
F	T	F	F	T
F	F	T	F	F

We see that the only time the expression is False is when both  $A$  and  $B$  are False, hence this expression is logically equivalent to  $A \vee B$ .

24. Find the negations of the following statements:

(a)  $(A \vee B) \wedge (B \vee C)$

(b)  $A \implies (B \wedge C)$

(c)  $\forall x \exists y (P(x) \vee (\text{not } Q(y)))$

**Solution.**  $\text{not}((A \vee B) \wedge (B \vee C)) \equiv \text{not}(A \vee B) \vee \text{not}(B \vee C) \equiv (\text{not}A \wedge \text{not}B) \vee (\text{not}B \wedge \text{not}C)$

$$\text{not}(A \implies (B \wedge C)) \equiv \text{not}(\text{not}A \vee (B \wedge C)) \equiv A \wedge \text{not}(B \wedge C) \equiv A \wedge (\text{not}B \vee \text{not}C)$$

$$\text{not}(\forall x \exists y (P(x) \vee (\text{not } Q(y)))) \equiv \exists x \forall y (\text{not}P(x)) \wedge Q(y)$$