Math 347: Practice for Final Exam
Dec. 12, 2018

1. Let $n \geq 2$ be a natural number.

   a) Assume n is a prime number. Prove that $x^2 \equiv 1 \bmod n$ if and only if $x \equiv 1 \bmod n$ or $x \equiv n-1 \bmod n$.

   Solution. *If $x \equiv 1 \; mod\, n$ or $x \equiv n-1$, one clearly has*

   $$x^2 \equiv 1^2 \equiv 1, \quad \textit{or} \quad x^2 \equiv (n-1)^2 \equiv n^2 - 2n + 1 \equiv 1 \; mod\, n.$$

   Conversely, let $x^2 \equiv 1 \; mod\, n$, we obtain

   $$x^2 - 1 \equiv 0, \Rightarrow \; (x-1)(x+1) \equiv 0.$$

   Now we want to say that for two numbers $a, b \in \mathbb{Z}$, if $ab \equiv 0$ modulo n, then $a \equiv 0$ modulo n or $b \equiv 0$ module n. This is only *true if n is prime. Since if a prime number p divides ab, then either p divides a or p divides b.*

   Thus, since n is prime the equation $(x-1)(x+1) \equiv 0 \; mod\, n$ implies

   $$x - 1 \equiv 0 \; mod\, n, \quad orx + 1 \equiv 0 \; mod\, n,$$

   which is what we wanted to prove. Notice $-1 \equiv n-1 \; mod\, n$.

   b) Does a) still hold if n is not a prime number? Prove your statement or give a conterexample.

   Solution. *No, it doesn't hold. If $n = 8$, then $5^2 \equiv 1$ modulo 8, but $5 \neq 1$ or 7.*

   The point that fails is exactly the claim in the middle paragraph in the above solution.

   c) Two siblings were born exactly 15 months apart. Knowing that *before a leap year* their birthday happens on the same day of the week, find out on which months they could have been born.

   Solution. *First we notice that $15 \equiv 3 \mod 12$, and since two years before a leap year is not a leap year, thus we can think of the birthdays as 3 months apart.*

   Second we calculate the value of the number of days of each month modulo 7 (since there are 7 days in a week). We have: Jan. 3, Feb 0 or 1 (if leap year), Mar. 3, April 2, May 3, Jun 2, July 3, August 3, Sep. 2, Oct. 3, Nov. 2 and Dec. 3.

   Third we notice that since the days of the week don't change in any years, it means that between the birthdays (recall we are considering that they are 3 months apart) there is no month of February.

   Fourth, we calculate the possible sums, always modulo 7, of days for three consecutive months, non-including Feb. We have: Mar.-May 1, Apr.-Jun. 0, May.-July. 1, Jun.-Aug. 1, July.-Sep.1, Aug.-Oct. 1, Sep.-Nov. 0, Oct.-Dec. 1 and Nov.-Jan. 1.

   We conclude that their birthdays are either in April and July, or September and December.

2. Let (a_n) be a Cauchy sequence, and (b_n) a subsequence such that $\lim b_n = L$. Prove that $\lim a_n$ exists and is equal to L.

   Solution. *Let $\varphi : \mathbb{N} \to \mathbb{N}$ be a strictly increasing function such that*

   $$b_n = a_{\varphi(n)}.$$

   By assumption, i.e. that $\lim b_n = L$, we know that for every $\epsilon > 0$, there exists $N_1 \in \mathbb{N}$ such that for all $n \geq N_1$ we have

   $$|b_n - L| < \epsilon/2.$$

   Also, because (a_n) is Cauchy, we know that for every $\epsilon > 0$, there exists $N_2 \in \mathbb{N}$ such that for all $n, m \geq N_2$ we have

   $$|a_n - a_m| < \epsilon/2.$$

Let $N = \max\{N_1, N_2\}$, we know that for any $n \geq N$, we have

$$|a_n - L| = |a_n - b_n + b_n - L| \leq |a_n - a_{\varphi(n)}| + |a_{\varphi(n)} - L| < \epsilon/2 + \epsilon/2 = \epsilon,$$

where the first inequality above comes from the triangle inequality, and the second by the fact that $\varphi(n) \geq n \geq N_1$ and $n \geq N_2$.

Thus, $\lim a_n = L$.

3. a) Let $a, b \in \mathbb{N}$ such that $\gcd(a, b) = 1$. Prove that there exist n and m such that

$$na + mb = 1.$$

Solution. *First we notice that for any $a, b \in \mathbb{Z}$ we have*

$$\gcd(a, b) = \gcd(a, -b) = \gcd(-a, b) = \gcd(-a, -b).$$

Thus, it is enough to consider $a, b \in \mathbb{N}$. The base case is $a + b = 1$, by inspection we have

$$1 \cdot 1 + 0 \cdot 0 = 1, \quad \textit{for the case } a = 1 \textit{ and } b = 0,$$

and

$$0 \cdot 0 + 1 \cdot 1 = 1, \quad \textit{for the case } a = 0 \textit{ and } b = 1.$$

Let's assume by strong induction that we proved the result for all pairs $(a, b) \in \mathbb{N}^2$ such that $a + b = k$, for some $k \geq 1$
Consider a pair (a', b') such that $a' + b' = k + 1$. Notice that a' and b' are both bigger than or equal to 1[1]*.*
Let $c = \max\{a', b'\}$ and $d = \min\{a', b'\}$, notice we have $c - d > 0$[2]*. Now consider the pair $(d, c - d)$. Since we have*

$$d + c - d = c < k + 1,$$

since $a \geq 1$ and $b \geq 1$. By the inductive hypothesis, there exists $(m, n) \in \mathbb{Z}^2$ such that

$$md + n(c - d) = 1 \quad \Rightarrow \quad (m - n)d + nc = 1.$$

In other words, we prove that there are integers $m', n' \in \mathbb{Z}^2$[3] *such that*

$$m'a + n'b = 1.$$

This finishes of the inductive step, hence of the whole proof.

b) Suppose that $\gcd(a, b)$ divides c. Does the equation

$$ax + by = c.$$

have integers solutions $(x, y) \in \mathbb{Z} \times \mathbb{Z}$?

Solution. *Let $d = \gcd(a, b)$ and consider $\frac{a}{d}$ and $\frac{b}{d}$. First we notice that $\gcd(\frac{a}{d}, \frac{b}{d}) = 1$*[4]*.*
Now, we know that there exists $n, m \in \mathbb{Z}$ such that

$$\frac{a}{d}m + \frac{b}{d}n = 1.$$

Multiplying the above equation by d we obtain a solution.

[1]Indeed, if $a' = 0$ one has $b' = k + 1 \geq 2$ and $\gcd(a', b') = k + 1 > 1$, thus a contradiction.

[2]Again, otherwise this is a contradiction with $\gcd(a, b) = 1$.

[3]Namely, $m' = m - n$ and $n' = n$ if $a < b$, and $m' = n$ and $n' = m - n$ otherwise.

[4]Indeed, by contradiction if $e > 1$ is their greatest common divisor we can write $a = ked$ and $b = \ell ed$ for some $k, \ell \in \mathbb{Z}$, thus contradicting that $d = \gcd(a, b)$.

c) Let $(x_0, y_0) \in \mathbb{Z} \times \mathbb{Z}$ be a solution to

$$ax + by = c.$$

Write all the solutions to the equation above in terms of x_0, y_0, a, b and $d = \gcd(a, b)$.

Solution. *By b) we know that a solution (x_0, y_0) exists. Let (x_1, y_1) be another solution, we compute that*

$$a(x_1 - x_0) + b(y_1 - y_0) = 0. \tag{1}$$

Since d divides a and b we can divide the above equation and manipulate it to obtain

$$\frac{a}{d}(x_1 - x_0) = -\frac{b}{d}(y_1 - y_0).$$

Now, notice that because $\gcd(\frac{a}{d}, \frac{b}{d}) = 1$, we have that

$$\frac{a}{d} \text{ divides } y_1 - y_0, \quad \text{and} \quad \frac{b}{d} \text{ divides } x_1 - x_0.$$

This implies that there exists $k, \ell \in \mathbb{Z}$ such that

$$x_1 = x_0 + k\frac{b}{d}, \quad \text{and} \quad y_1 = y_0 + \ell\frac{a}{d}.$$

Substituing these back into (1) gives

$$\frac{ab}{d}k + \frac{ab}{d}\ell = 0.$$

This implies that $\ell = -k$.

As the solutions (x_0, y_0) and (x_1, y_1) were arbitrary, this proves that the set S of solutions is given by

$$S = \{(x_0 + k\frac{b}{d}, y_0 - k\frac{b}{d}) \mid k \in \mathbb{Z}\}.$$

4. a) Let S be a finite set and $f : S \to S$ an injective function. Prove that f is surjective.

Solution. *First we notice that if $f : A \to B$ is an injective function between finite sets, then B has as many elements as A.*

Suppose f is not surjective and let $s \in S$ be such that for all $t \in S$, $f(t) \neq s$. Then one has a well-defined function

$$g : S \to S \backslash \{s\},$$

given by $g(x) = x$ for all $x \in S$, and g is also injective. However, the previous paragraph implies that $S\backslash\{s\}$ has as many elements as S, which is a contradiction.

b) Give an example of a set S where the above conclusion fails[5].

Solution. *Consider $S = \mathbb{Z}$ and $f(n) = 2n$. This is injective since $2n = 2m$ implies that $n = m$, for $n, m \in \mathbb{Z}$. But 1 is not in the image of f.*

c) Let T be a set such that there exists an injective function $g : T \to \mathbb{N}$. What can you say about the cardinality[6] of T.

Solution. *If g is also surjective, we know that T is countable. If it is not surjective, then T can be finite[7], but it can also be countable, as the example in b) shows.*

5. Let S be the set of sequences of non-zero real numbers, i.e. functions from $\mathbb{N}$ to $\mathbb{R}\backslash\{0\}$. Consider the relation R on S,

$$((a_n), (b_n)) \in R, \text{ if } \forall \epsilon \in \mathbb{R}_{>0},\ \exists N \in \mathbb{N}, \text{ s.t. } \forall n \geq N,\ |a_n - b_n| < \epsilon.$$

[5] Namely, where an injective function from S to S is not necessarily surjective.

[6] Be precise in your answer, if necessary recall what we defined about any words you use.

[7] Recall that we defined a set to be countable if it is in bijection with $\mathbb{N}$.

a) Prove that R is an equivalence relation.

Solution. *First we notice that* $((a_n),(b_n)) \in R$ *if and only if*

$$\lim(a_n - b_n) = 0.$$

Let's now check the properties that are required for R *to be an equivalence relation.*
Reflexive, we notice that $\lim a_n - a_n = 0$*, so* $((a_n),(a_n)) \in R$.
Symmetric, we notice that if the limit $\lim(a_n - b_n)$ *exists, then* (-1) *times it also exists and is equal to*

$$\lim(b_n - a_n) = \lim(-1)(a_n - b_n) = (-1)\lim(a_n - b_n) = 0.$$

Thus, if $((a_n),(b_n)) \in R$*, then* $((b_n),(a_n)) \in R$.
Transitive, suppose that $((a_n),(b_n)) \in R$ *and that* $((b_n),(c_n)) \in R$*, then the limits*

$$\lim(a_n - b_n), \quad \textit{and} \quad \lim(b_n - c_n)$$

both exist and are equal to 0*. We can then consider the limit of the sum*

$$\lim(a_n - b_n + b_n - c_n) = \lim(a_n - c_n),$$

which by results we proved in the course is the same as the sum of the limits, hence 0*. Thus* $((a_n),(c_n)) \in R$.

b) Give three examples of sequences in the equivalence class of $a_n = \frac{1}{n^2}$.

Solution. *The sequences* $b_n = \frac{1}{n}$, $c_n = \frac{(-1)^n}{n^2}$ *and* $d_n = \frac{1}{n^4}$ *are all in the equivalence class of* a_n.

c) Prove that $a_n = \frac{(-1)^n}{n}$ and $b_n = \frac{1}{n}$ are in the same equivalence class.

Solution. *We need to prove that*

$$\lim \frac{(-1)^n}{n} - \frac{1}{n}$$

is 0.
Let $\epsilon > 0$*, by the Archimidean property, there exists* $N \in \mathbb{N}$ *such that* $\frac{1}{N} < \frac{\epsilon}{2}$*. Thus, for any* $n \geq N$ *we have*

$$|\frac{(-1)^n}{n} - \frac{1}{n}| \leq \frac{2}{n} < \epsilon,$$

which proves by the definition that the limit vanishes.

6. a) For $n \geq 1$, prove that[8]

$$\sum_{i=0}^{n} \binom{i}{k} = \binom{n+1}{k+1}.$$

Solution. *For every* n*, we will perform a "reverse" induction on* k*, that is we will prove the result for a base case, and that if it holds for* $k \geq 1$ *then it holds to* $k-1$.
Base case: $k = n$ *we have*

$$\binom{n}{n} = \binom{n+1}{n+1}.$$

Inductive case: suppose the result holds for some k *such that* $1 \leq k \leq n$*. Then consider*

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

[8]If $a < b$ we define

$$\binom{a}{b} = 0.$$

by Pascal's identity, and in the two sums all the terms cancels, except for

$$\binom{n+1}{k}.$$

Thus, the result is also valid for $k-1$.

As this argument works for any n*, this finishes the proof.*

b) Find the number of non-negative integer solutions to

$$x_1 + x_2 + \cdots + x_k \leq n.$$

Solution. *Let* $x_{k+1} = n - \sum_{i=1}^{k} x_i \geq 0$. *So, one has that the number of non-negative* $x_1, \ldots, x_k$ *satisfying the desired equation, is the same as the numbers of* $x_1, \ldots, x_k, x_{k+1}$ *which satisfy the equation*

$$x_1 + \cdots + x_k + x_{k+1} = n.$$

This number we calculated before, see Worksheet 10 exercise 3 and is given by[9]

$$\binom{n+k}{k}.$$

7. Give examples of the following structures or argue why no example exists. You also need to explain why your examples satisfy the required properties.

a) A set S and a relation R, that is symmetric and reflexive but not transitive.

Solution. *Consider the set* $S = \mathbb{Z}$ *and the relation is* $(x, y) \in R$ *if*

$$\gcd(x, y) = 1.$$

It is not transitive, as the pairs $(2, 3)$ *and* $(3, 4)$ *show.*

b) A set S and a relation R, that is reflexive, transitive and anti-symmetric, i.e. if $(x, y) \in R$ and $(y, x) \in R$, then $x = y$.

Solution. *Consider* $S = \mathbb{Z}$ *and the relation* $(x, y) \in R$ *if* $x \leq y$.

We notice that $x \leq y$ *and* $y \leq x$*, implies that* $x = y$.

c) An equivalence relation R on $\mathbb{Z}$ that has finitely many equivalence classes and an equivalence relation R' that has infinitely many equivalence classes.

Solution. *We can take for* R *the equivalence relation* $(x, y) \in R$ *if* $x - y$ *is divisible by* 3. *This equivalence relation has* 3 *equivalence classes, namely the residues of division by* 3.

We can take for R' *the equivalence relation* $(x, y) \in R$ *if* $|x| = |y|$. *We notice that there are* $\mathbb{Z}_{\geq 0}$ *different equivalence relations with respect to* R'. *Namely, for any* $n \in \mathbb{Z}_{\geq 0}$*, one has*

$$[n] = \{n, -n\}, \quad \text{if } n \neq 0,$$

and $[0] = \{0\}$.

d) Two functions f and g, such that $g \circ f$ is surjective but f is not surjective.

Solution. *Consider the functions* $f : \mathbb{Z}_{\geq 0} \to \mathbb{Z}$ *and* $g : \mathbb{Z} \to \mathbb{Z}_{\geq 0}$ *given by*

$$f(x) = x, \quad \text{and} \quad g(x) = |x|.$$

The composite $g \circ f(x) = x$*, which is clearly surjective. However,* f *is not surjective, since the number* $-1 \in \mathbb{Z}$ *is not in the image of* f.

[9] Recall, the argument is that we are counting the number of ways to arrange n balls and k bars separating them, namely the number of ways to choose k bars among $n+k$ symbols.

e) A non-monotone Cauchy sequence.

Solution. *Consider the function* $x_n = \frac{(-1)^n}{n}$. *It is a convergent sequence, hence it is also Cauchy. And it is clearly not monotone, since it has changing sign.*

We can also directly check that x_n *is Cauchy. Let* $\epsilon > 0$, *by the Archimedian property, there exists* $N \in \mathbb{N}$ *such that* $\frac{1}{N} < \frac{\epsilon}{2}$. *Now for any* $n, m \geq N$ *we have*

$$|\frac{(-1)^n}{n} - \frac{(-1)^m}{m}| \leq \frac{2}{\min\{n,m\}} < \epsilon,$$

which is what we needed to check.

f) Sets A, B, a function $f : A \to B$, and a subset $T \subseteq B$, such that

$$f(f^{-1}(T)) \neq T.$$

Solution. *Consider the set* $B = \{0,1\}$ *and any set* A. *We define the function* $f : A \to \{0,1\}$ *to be the constant function that takes all the elements of* A *to* 0. *Let* $T = \{1\}$. *Then* $f^{-1}(T) = \emptyset$, *and* $f(f^{-1}(T)) = f(\emptyset) = \emptyset \neq T$.

g) Non-trivial sets A, B and C such that

$$(A \cap B) \cup C = A \cap (B \cup C).$$

Solution. *Consider* $A = B = C$, *then both sides are* A.

h) Sets S such that the set of functions $X \to S$ has the same cardinality as $P(X)$, the power set of X.

Solution. *If* S *has two elements, then the set of functions* $f : X \to S$ *has cardinality* $2^|X|$, *hence the same cardinality of* $P(S)$. *Thus any set with two elements will do, for example*

$$S = \{T, F\}, \quad S = \{0,1\}, \quad \textit{or} \quad S = \{\textit{cat}, \textit{dog}\}.$$

8. Determine if the following are true or false, and give a brief explanation.

a) The statements

$$(P \Rightarrow (Q \wedge \neg Q)) \Rightarrow \neg P$$

and

$$P \vee \neg P$$

are logically equivalent.

Solution. *We recall that* $P \Rightarrow Q$ *is equivalent to* $\neg P \vee Q$. *Thus, we can rewrite the first phrase as*

$$\neg((\neg P \vee (Q \wedge \neg Q))) \vee \neg P.$$

Distributing the outmost $\neg$ *we get*

$$(P \wedge \neg(Q \wedge \neg Q)) \vee \neg P.$$

We notice that $\neg(Q \wedge \neg Q)$ *is always true, since it has a* $\wedge$ *attached to it, we can drop it, hence obtaining*

$$P \vee \not P,$$

which is always true.

So the two statements are equivalent.

b) Fix $a, L \in \mathbb{R}$ and a function $f : \mathbb{R} \to \mathbb{R}$. Consider the statements

$$P = (\forall \epsilon)\ (\exists \delta > 0)\ (\forall x \in \mathbb{R})\ [(0 < |x - a| < \delta) \Rightarrow (|f(x) - L| < \epsilon),$$

and

$$Q = (\exists \delta > 0)\ (\forall \epsilon)\ (\forall x \in \mathbb{R})\ [(0 < |x - a| < \delta) \Rightarrow (|f(x) - L| < \epsilon).$$

Then $Q \Rightarrow P$.

Solution. *Statement P is saying that* $\lim_{x\to a} f(x) = L$.
Statement Q is stating that for all $x \in (a-\delta, a+\delta)\setminus\{a\}$ we have

$$f(x) = L.$$

Thus, Q implies P.
The converse is not true, though, consider $f(x) = b(x-a) + L$, for any $b \neq 0$.

c) For any $n \in \mathbb{Z}$ and any $b \in \mathbb{Z}\setminus\{0\}$, there exists an unique pair $(q, r) \in \mathbb{Z} \times \mathbb{Z}$ such that

$$n = bq + r.$$

Solution. *This is not true. For $n = 10$, $b = 5$ we have*

$$10 = 2 \cdot 5 = 1 \cdot 5 + 5.$$

In the first equation we have the pair $(q, r) = (2, 0)$ in the second $(q', r') = (1, 5)$.
The statement that is true, is that those numbers are unique, if we impose that $0 \leq r \leq b - 1$.

d) Let $n, a \in \mathbb{N}$. Consider the statements

$$P = (\exists x \in \mathbb{N})(a + x \equiv 1 \bmod n),$$

and

$$Q = ([a]+ : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} \text{ is surjective.})^{10}.$$

Then $Q \Rightarrow P$ is false.

Solution. *Suppose that Q is true. Consider $[1] \in \mathbb{Z}/n\mathbb{Z}$, since $[a]+$ is surjective, this implies that there exists $[x] \in \mathbb{Z}/n\mathbb{Z}$ such that*

$$[a] + [x] = [1],$$

in other words

$$a + x \equiv 1 \ mod\, n.$$

That is, there exists $x \in \mathbb{Z}$ such that the above equation is satisfied. Notice, that we can make $x \in \mathbb{N}$ by picking a sufficiently large number $k \in \mathbb{N}$ and considering

$$x' = x + k \cdot n.$$

And we will still have

$$a + x' \equiv a + x + k \cdot n \equiv a + x \equiv 1 \ mod\, n.$$

e) The statement

$$(\forall n \in \mathbb{N})(\gcd(n, n+3) = 1)$$

is true.

Solution. *No, consider $n = 3$, we have*

$$\gcd(3, 6) = 3 \neq 1.$$

More generally, we know that if d divides n and $n + 3$, then d divides

$$(n + 3) - n = 3.$$

Thus, $\gcd(n+3, n) = \gcd(n, 3)$. *So any time that n is not divisible by 3 the greatest common divisor between n and $n + 3$ is 1.*

f) Let $A \subset B$ be two finite sets. Suppose that there are 4 subsets of B containing A. Then $|A| = |B| - 2$.

[10] Recall that this function is explicitly defined as $[a] + [x] = [a + x]$, for any $[x] \in \mathbb{Z}/n\mathbb{Z}$.

Solution. *Suppose that B has n elements and A has k elements. We see that there are*

$$\binom{\sum_{i=0}^{n-k}}{n-ki = 2^{n-k}.}$$

choices of subsets that contain A. Thus, we want

$$n-k=4,$$

which gives that $|B|-|A|=2$, thus proving the result.