

MATH113 SOLUTIONS: HOMEWORK 1

- (1) §1.2 #15 For any finite set, X , let $m(X)$ denote the number of elements in X . Use the results from §1.2 #1-12 and especially #14 to derive a formula for $m(A \cup B \cup C)$ in terms of the number of elements in the finite sets A , B and C , and their intersections.

Solution: We'll use the result from #9 that $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$, as well as the result from #14 that $m(A \cup B) = m(A) + m(B) - m(A \cap B)$

$$\begin{aligned}
 & m(A \cup B \cup C) \\
 = & m(A \cup [B \cup C]) \\
 = & m(A) + m([B \cup C]) - m(A \cap [B \cup C]) && \text{(by #14)} \\
 = & m(A) + [m(B) + m(C) - m(B \cap C)] - m([A \cap B] \cup [A \cap C]) && \text{(by #14, 9)} \\
 = & m(A) + m(B) + m(C) - m(B \cap C) - [m(A \cap B) + m(A \cap C) - m(A \cap B \cap C)] && \text{(#14)} \\
 = & m(A) + m(B) + m(C) - m(A \cap B) - m(A \cap C) - m(B \cap C) + m(A \cap B \cap C)
 \end{aligned}$$

- (2) Consider a function $f : S \rightarrow T$ for any $C \subseteq S$, we define a certain subset of T , the **image of C under f** , as $f(C) := \{f(c) : c \in C\}$.

- (a) Let $A, B \subseteq S$. Show that $f(A \cup B) = f(A) \cup f(B)$.

Keep in mind that the left and right hand sides of this equation are SETS. The usual way to show that two sets are equal is to show that the LHS is contained in the RHS and viceversa.

Solution: Let $y \in \text{LHS} = f(A \cup B)$. Then there is an x in $A \cup B$ with $f(x) = y$. By definition of $A \cup B$, there are two cases to consider: Either $x \in A$, hence $y \in f(A)$; or $x \in B$, hence $y \in f(B)$. Thus $y \in f(A) \cup f(B) = \text{RHS}$. We just showed that $y \in \text{LHS} \implies y \in \text{RHS}$. Therefore, $\text{LHS} \subseteq \text{RHS}$.

In the other direction, let $y \in \text{RHS} = f(A) \cup f(B)$. By the definition of union, there are two cases: Either $y \in f(A)$, in which case there exists $x \in A$ with $f(x) = y$; or $y \in f(B)$, in which case there exists $x \in B$ with $f(x) = y$. In either case, $x \in A \cup B$, and hence $y \in f(A \cup B) = \text{LHS}$.

We just showed that $y \in \text{RHS} \implies y \in \text{LHS}$. Therefore, $\text{RHS} \subseteq \text{LHS}$. Since we have shown that each side of the equation is contained in the other, the two sets are equal. Therefore $f(A \cup B) = f(A) \cup f(B)$.

- (b) Let $A, B \subseteq S$. Show that $f(A \cap B) \subseteq f(A) \cap f(B)$, and give an example to show that the left and right sides need not be equal.

Solution: Let $y \in f(A \cap B)$. Then there exists $x \in A \cap B$ with $f(x) = y$. By the definition of $A \cap B$, $x \in A$ (hence $y \in f(A)$), AND $x \in B$ (hence $y \in f(B)$). Therefore, by the definition of intersection, $y \in f(A) \cap f(B)$. (We have just shown $y \in f(A \cap B) \implies y \in f(A) \cap f(B)$.) So we have shown $f(A \cap B) \subseteq f(A) \cap f(B)$.

Consider the function $f : \mathbb{R} \rightarrow \mathbb{R}$ given by $f(x) = x^2$, and let A be the set of *positive* numbers $A = \{x > 0\}$, and B the set of *negative* numbers $B = \{x < 0\}$. Then $A \cap B$ is empty, and therefore so is $f(A \cap B)$. On the other hand, $f(A) \cap f(B)$ is certainly not empty, since, for example, $4 = 2^2 = f(2) \in f(A)$ and $4 = (-2)^2 \in f(B)$, so $4 \in f(A) \cap f(B)$. In fact, $f(A) \cap f(B) = \{x > 0\}$. So this is a good example of $f(A \cap B) \neq f(A) \cap f(B)$. Of course, there are many other examples that work.

- (3) §1.3 #6 If $f : S \rightarrow T$ is onto, and $g : T \rightarrow U$ and $h : T \rightarrow U$ are such that $g \circ f = h \circ f$, prove that $g = h$.

Remember that the best way to show that two functions are equal is to show that "they agree on every element of their domain".

Solution: Let $t \in T$. f is onto, so there is an $s \in S$ with $f(s) = t$, and:

$$g(t) = g(f(s)) = g \circ f(s) = h \circ f(s) = h(f(s)) = h(t)$$

(We have just showed that for all $t \in T, g(t) = h(t)$.) Therefore $g = h$.

- (4) §1.3 #7 If $f : T \rightarrow U$ is 1-1 and $g : S \rightarrow T$ and $h : S \rightarrow T$ are such that $f \circ g = f \circ h$, prove that $g = h$.

This one is a little trickier than the last, but the idea is the same. We need to show that g and h agree on every element of S .

Solution: Let $s \in S$. Since $f \circ g = f \circ h$, we know that

$$f(g(s)) = f \circ g(s) = f \circ h(s) = f(h(s))$$

but f is 1-1, so $f(g(s)) = f(h(s)) \implies g(s) = h(s)$. (We have just shown that $g(s) = h(s)$ for all $s \in S$.) Therefore $g = h$.

- (5) Let $f : S \rightarrow T$ and $g : T \rightarrow U$.

- (a) If $g \circ f$ is onto, show that g must be onto, but f need not be.

Solution: Let $u \in U$. Since $g \circ f$ is onto, there is an $s \in S$ with $u = g \circ f(s) = g(f(s))$. Let $t = f(s)$. Then $g(t) = u$. (We have just shown that for any $u \in U$ there is a t with $g(t) = u$.) Therefore g is onto. See part (c) for an example which shows that f doesn't have to be onto, even if $g \circ f$ is.

- (b) If $g \circ f$ is 1-1, show that f must be 1-1 but g need not be.

Solution: The goal is to show that $f(s_1) = f(s_2) \implies s_1 = s_2$, so we start by assuming that $f(s_1) = f(s_2)$ and trying to show that this forces $s_1 = s_2$. Suppose we have $f(s_1) = f(s_2)$. Then

$$g \circ f(s_1) = g(f(s_1)) = g(f(s_2)) = g \circ f(s_2)$$

We know that $g \circ f$ is 1-1, thus we know that $g \circ f(s_1) = g \circ f(s_2) \implies s_1 = s_2$. Therefore $s_1 = s_2$ by injectivity of $g \circ f$. Thus f is 1-1. See part (c) for an example that shows that g doesn't have to be injective, even if $g \circ f$ is.

- (c) Give an example of two non-invertible functions whose composition is invertible.

Solution: Consider $S = \{1\}$, $T = \{2, 3\}$, $U = S$. And let f be the function $f(1) = 2$, and g the function $g(2) = g(3) = 1$. Then it is clear that f is not onto – since 3 is not in the image of f . Also, g is not injective, since the two distinct elements, 2 and 3 are sent to the same place, namely 1. On the other hand, $g \circ f : S \rightarrow U$ is just identity function on S , and thus invertible (it is its own inverse). This example has small sets and simple functions to show exactly what can go wrong: g can have lots of “non-injective” behavior on the part of T that f misses, and f can hit enough of T that $g \circ f$ is onto – it doesn't have to hit the “redundant” parts of T where g repeats values.

- (6) Let $\sigma = (1452)$ and $\tau = (23)(45)$ be permutations in S_5 . Calculate, and express in cycle notation:

- (a) $\sigma^2, \sigma^3, \sigma^4, \sigma^5$

$$\sigma^2 = \sigma^5 = (15)(24), \sigma^3 = (1245), \sigma^4 = (1)(2)(3)(4) = e$$

- (b) τ^2, τ^3

$$\tau^2 = (2)(3)(4)(5) = e, \tau^3 = (23)(45)$$

- (c) $\sigma\tau, \tau\sigma$

I'll explain the product $\sigma\tau$ in detail as an example of how to do these in general. Since we're writing the solution in cycle notation, start by writing the first number you're going to study – an obvious choice is 1, so we start writing “1”. The number we write next should be the image of 1 under the composition $\sigma\tau$ – don't forget that this means we apply τ first. τ doesn't change 1, and σ sends 1 to 4, so we continue writing “(14”. The next number to write down is the place we send 4 to under the composition. τ sends 4 to 5 and σ sends 5 to 2, so the composition sends 4 to 2, so we continue writing “(142”. Next consider where $\sigma\tau$ sends 2. τ sends 2 to 3, and σ doesn't change 3, so we continue “(1423”. Now we ask where $\sigma\tau$ sends 3: τ sends 3 to 2, and σ sends 2 to 1. So we would write 1 as the next number, but since it's the first one in the brackets, we just close the cycle we're working on: “(1423)”. Since we've closed the current cycle, we need to start a new one, with a number we haven't looked at yet: the obvious choice is 5, so we continue: “(1423)(5)”. You can check for yourself that $\sigma\tau$ sends 5 to itself, so we close that cycle: “(1423)(5)” and there aren't any more numbers involved in σ or τ , so we're done. There's no need to write the singleton cycles, so we can leave off the (5).
 $\sigma\tau = (1423), \tau\sigma = (1532)$

- (d) σ^{-1}
 σ^{-1} is the permutation that thinks about where σ sends every number, and sends it back to where it came from. For example, σ sends 1 to 4, so σ^{-1} must send 4 back to 1! If you think for a moment, you'll see that this means that the inverse of a cycle is just the "reverse" cycle. So why didn't I ask you to calculate τ^{-1} ?
 $\sigma^{-1} = (2541)$ Of course, you might write (1254) instead.
- (e) $\sigma\tau\sigma^{-1}$
 $\sigma\tau\sigma^{-1} = (1452)(23)(45)(1254) = (13)(25)$ You can either solve this one by multiplying out the cycles as in the comments for part (c), or by applying question (7). Try to see how this second method works, because we'll come back to it later in the semester.

- (7) Let $\sigma = (a_1 a_2 \dots a_k)$ be a cycle, and τ any permutation in S_n with $(n \geq k)$. Show that

$$\tau\sigma\tau^{-1} = (\tau(a_1) \tau(a_2) \dots \tau(a_k))$$

Solution: This is very straightforward once you decipher all the nonsense. Let LHS and RHS be the left and right hand sides of the equation above that we are trying to prove. The important thing to remember is that $\tau(a_1)$, for example, is a NUMBER. And the RHS of the equation is a function that sends $\tau(a_1)$ to $\tau(a_2)$ So where does LHS = $\tau\sigma\tau^{-1}$ SEND $\tau(a_1)$?

Just evaluating the composition, we see that

$$\tau\sigma\tau^{-1}(\tau(a_1)) = \tau(\sigma(a_1)) = \tau(a_2)$$

The exact same calculation shows $\tau\sigma\tau^{-1}$ sends $\tau(a_i)$ to $\tau(a_{i+1})$ for $i = 1, 2, \dots, k-1$, and $\tau(a_k)$ to $\tau(a_1)$. This is exactly what the RHS says. Since τ is a bijection, we can write any number in $\{1, 2, \dots, n\}$ as $\tau(x)$ for some x . We just saw that the functions on the LHS and RHS agree on all the numbers of the form $\tau(a_i)$. What about the numbers of the form $\tau(x)$ for $x \notin \{a_1, \dots, a_k\}$? Those numbers are clearly fixed by the RHS, since they don't appear in that cycle. And

$$\tau\sigma\tau^{-1}(\tau(x)) = \tau\sigma(x) = \tau(x)$$

since x is not one of the a_i . Therefore the LHS fixes $\tau(x)$. The LHS and RHS therefore agree on every number in $\{1, 2, \dots, n\}$, so they're equal functions, which is what we're trying to prove.

- (8) §1.5 #1 Find (a, b) , and express (a, b) as $ma + nb$.
 You can probably just guess/factor that the gcds of these two pairs are 5 and 1, but since we have to express the gcd in a particular form, we will need to use the Euclidean algorithm.

- (b) $(85, 65)$

See part (b) for a fuller explanation.

$$\begin{array}{rcl} 85 & = & 1 \cdot 65 + 20 \quad (A) \\ 65 & = & 3 \cdot 20 + 5 \quad (B) \\ 20 & = & 4 \cdot 5 + 0 \quad (C) \end{array} \quad \left| \quad \begin{array}{rcl} 5 & = & 65 - 3 \cdot 20 \quad (B) \\ & = & 65 - 3 \cdot (85 - 1 \cdot 65) \quad (A) \\ & = & 4 \cdot 65 - 3 \cdot 85 \\ & = & 4 \cdot 65 + (-3) \cdot 85 \end{array} \right.$$

So the gcd is 5

(The last non-zero remainder). So $n = 4$ and $m = -3$.

- (d) $(72, 25)$

The key thing is to be totally methodical about how you write the equations from the division algorithm, so that you can keep track of which numbers are the quotient and the remainder.

$$\begin{array}{rcl} 72 & = & 2 \cdot 25 + 22 \quad (A) \\ 25 & = & 1 \cdot 22 + 3 \quad (B) \\ 22 & = & 7 \cdot 3 + 1 \quad (C) \\ 3 & = & 3 \cdot 1 + 0 \end{array}$$

Note that the divisor and the remainder become the dividend and divisor for the next.

The gcd is 1, the last non-zero remainder.

$$\begin{array}{rcl} 1 & = & 22 - 7 \cdot 3 \quad (\text{Rearranging (C)}) \\ & = & 22 - 7 \cdot (25 - 1 \cdot 22) \quad (\text{Use (B) to substitute for "3"}) \\ & = & 8 \cdot 22 - 7 \cdot 25 \quad (\text{Simplify by collecting like-terms; don't multiply too much out!}) \\ & = & 8 \cdot (72 - 2 \cdot 25) - 7 \cdot 25 \quad (\text{Use (A) to substitute for "22"}) \\ & = & 8 \cdot 72 - 23 \cdot 25 \quad (\text{Simplify: don't multiply too much!}) \end{array}$$

Therefore, $m = 8$

and $n = -23$.

- (9) (a) §1.5 #13(a) Show that every odd prime number is either of the form $4n + 1$ or $4n + 3$ for some integer n .

Solution: Claim: every integer is of the form $4n + i$ for $i = 0, 1, 2, 3$. This is a straight-up application of the division algorithm. Let $a \in \mathbb{Z}$. By the division algorithm, there exist q and r with $a = 4 \cdot q + r$ and $0 \leq r < 4$. Notice how important the bounds on r in the division algorithm are! Don't forget them! The q is our n , and the r is our i . Notice that $i \in \{0, 1, 2, 3\}$. Claim: Every prime is of the form $4n + 1$ or $4n + 3$. Let p be a prime number. Then $p = 4n + i$ for some $i \in \{0, 1, 2, 3\}$ by the previous claim. But we CAN'T have $p = 4n + 0 = 4n$, since this number is clearly not prime, and we CAN'T have $p = 4n + 2 = 2(2n + 1)$, since this number is clearly not prime. Thus $p = 4n + 1$ or $4n + 3$ for some $n \in \mathbb{Z}$ (notice it can't be both!).

- (b) Show by induction that for any m , the product of m integers of the form $4n + 1$ is also of that form.

BASE CASE: For $m = 1$, the statement is obviously true.

INDUCTION HYPOTHESIS: Assume the statement is true for some specific integer k .

INDUCTION STEP: Now the goal is to prove the statement is true for $m = k + 1$ by using the hypothesis above. Suppose we have integers $a_1, a_2, \dots, a_k, a_{k+1}$, and let $a_i = 4n_i + 1$. Then by the induction hypothesis,

$$\begin{aligned} a_1 a_2 \dots a_k &= 4N + 1 && \text{for some integer } N, \text{ and so} \\ a_1 a_2 \dots a_k a_{k+1} &= (4N + 1)a_{k+1} \\ &= (4N + 1)(4n_{k+1} + 1) \\ &= 16Nn_{k+1} + 4n_{k+1} + 4N + 1 \\ &= 4(4Nn_{k+1} + n_{k+1} + N) + 1 \end{aligned}$$

We just showed that IF we assume that the product of k numbers of the form $4n + 1$ is also of that form, THEN the product of $k + 1$ numbers of the form $4n + 1$ is also of that form. So the case $m = k + 1$ follows from the case $m = k$. By mathematical induction, the statement is true for all integers m .

- (c) §1.5 #14(a) Adapt Euclid's proof of the infinitude of primes (Th'm 1.5.9) to show that there is an infinite number of primes of the form $4n + 3$.

Solution: We'll prove the statement by contradiction. Which means we begin by assuming that the statement is FALSE, and showing that this leads to some logical contradiction. So the first step is to Assume that there are only finitely many primes of the form $4n + 3$. Now that we have made this assumption, let's name these primes so that we can use them: Let $3, p_1, p_2, \dots, p_s$ be a complete (and non-repeating) list of the primes of the form $4n + 3$. Note I kept 3 separate, because I'll need it later. If we were just copying Euclid's proof, we might try to invent a new prime $p_1 p_2 \dots p_s + 1$, but this new number may or may not be of the correct form, so let's instead invent a new number that we know is of the form $4n + 3$. Let $M = 4p_1 p_2 \dots p_s + 3$. Notice that M is not divisible by p_i for any i , and not divisible by 3 either. if it were, say divisible by p_1 , then there's a $k \in \mathbb{Z}$ with $k p_1 = M = 4p_1 p_2 \dots p_s + 3$ and hence $3 = p_1(k - 4p_2 \dots p_s)$, which is nonsense, since 3 is prime. Since the p_i 's are the only primes of the form $4n + 3$, by part(a) all of the primes in the factorization of M are of the form $4n + 1$. But by part (b) this means that M is of that form too, which is a contradiction since it's of the form $4n + 3$, not $4n + 1$. We derived this contradiction logically from the assumption that there are finitely many primes of the form $4n + 3$, so that assumption is false. Therefore there are infinitely many primes of the form $4n + 3$.

- (10) Complete the following table of values in the integers mod 11, with one column for each element of $\mathbb{Z}/11\mathbb{Z}$.

It doesn't matter how you filled out this table, as long as you know that there are some shortcuts! For example, don't do $6^4 = 1296$ and then try to figure out the remainder on division by 11. Instead, notice $6^4 = (6^2)^2 = 3^2 = 9$. If you finish the first row, you shouldn't need to do any multiplications to get the third row! Also, for example to find 9^2 the fastest way, notice that $9 = -2$ in $\mathbb{Z}/11\mathbb{Z}$, so $9^2 = (-2)^2 = 4$. This should help you find and explain the important pattern in the first and third rows.

Solution:

x	0	1	2	3	4	5	6	7	8	9	10
x^2	0	1	4	9	5	3	3	5	9	4	1
x^3	0	1	8	5	9	4	7	2	6	3	10
x^4	0	1	5	4	3	9	9	3	4	5	1

- (11) Solve the equation $13x \equiv 7 \pmod{29}$

We would love to be able to “divide both sides” by 13, but of course this will give us non-integer values for x . Instead, let's find a multiplicative inverse for 13 mod 29. We know such an inverse exists since $(13, 29) = 1$. We use the division algorithm:

$$29 = 2 \cdot 13 + 3 \quad (A)$$

$$13 = 4 \cdot 3 + 1 \quad (B)$$

$$1 = 13 - 4 \cdot 3 \quad \text{from } (B)$$

$$= 13 - 4(29 - 2 \cdot 13) \quad \text{from } (A)$$

$$= 9 \cdot 13 - 4 \cdot 29$$

Notice that this last line says: $9 \cdot 13 = 1 + 4 \cdot 29 \equiv 1 \pmod{29}$ Therefore 9 is a multiplicative inverse for 13 in “mod 29” land, and

$$13x \equiv 7 \pmod{29}$$

$$9 \cdot 13x \equiv 9 \cdot 7 \pmod{29}$$

$$x \equiv 5 \pmod{29}$$

The solution is that x can be any integer of the form $29k + 5$ for $k \in \mathbb{Z}$.