

- Show all answers and work in the blue books. Show all the work necessary to solve the problem.
- Each problem goes with a section (or more than one). You must cite every result you use (for that problem) in those sections (but not in other sections).

(1) (10 points) (Sect. 1.1–2) Prove that, if  $i|m$  and  $i|n$ , then  $i|(m - n)$ .

**Solution.** We know from the definition of divisibility that  $m = ji$  and  $n = ki$  for some integers  $j$  and  $k$ . (Note:  $m = ij$  is not the definition. This is Chapter 1; pay attention to the details.) Therefore,  $m - n = ji - ki$ . By Prop. ?? this =  $(j - k)i$ , which by the definition of divisibility means that  $i|(m - n)$ .

Using  $j$  for two different numbers is fatal.

(2) (5 points) (Sect. 1.1–2) For which integers  $m$  is it true that  $0|m$ ? (Prove.)

**Solution.**

(3) (10 points) (Sect. 2.2) Let  $x, y \in \mathbb{Z}$ . Prove that  $x, y > 1 \implies xy > 1$ .

**Solution.**

(4) (5 points) (Sect. 4.2) Assume there are numbers  $a_i$  for all  $i \in \mathbb{Z}$ . Write a correct definition of  $\sum_{i=m}^n a_i$  and state for which pairs  $(m, n)$  ( $m, n \in \mathbb{Z}$ ) your definition is valid.

Make this as many pairs as possible.

**Solution.** Definition:

$$\sum_{i=m}^n a_i = \begin{cases} a_m & \text{if } n = m, \\ \sum_{i=m}^{n-1} a_i + a_n & \text{if } n > m. \end{cases}$$

This definition is valid for all pairs  $(m, n)$  in which  $m \leq n$ .

Partial credit for defining only  $\sum_{i=1}^n a_i$ .

Nothing says what the value of  $a_i$  is. Assuming  $a_i = i$  is a major error.

(5) (10 points) (Sect. 3.1–3) Negate this logical statement; simplify the negation as much as possible:

All apples are sweet if and only if some bananas are green.

**Solution.** (This logic is expected for passing the class. You will see it again.)

The best way to do this is *one logical step at a time*. If you didn't, you probably got a bad result. The first step is to rewrite as two implications:

$$\begin{aligned} & ((\text{all apples are sweet}) \implies (\text{some bananas are green})) \text{ AND} \\ & ((\text{some bananas are green}) \implies (\text{all apples are sweet})). \end{aligned}$$

The next step is to negate the first operation, AND:

$$\begin{aligned} & [\text{NOT}((\text{all apples are sweet}) \implies (\text{some bananas are green}))] \text{ OR} \\ & [\text{NOT}((\text{some bananas are green}) \implies (\text{All apples are sweet}))]. \end{aligned}$$

Now comes the critical step: negate the implications.

$$\begin{aligned} & [((\text{All apples are sweet}) \text{ AND NOT}(\text{some bananas are green}))] \text{ OR} \\ & [((\text{some bananas are green}) \text{ AND NOT}(\text{all apples are sweet}))]. \end{aligned}$$

Finally, negate the two quantified expressions that require negation.

[(all apples are sweet AND all bananas are not green)] OR  
[(some bananas are green AND some apples are not sweet)].

“No bananas are green” means the same as “all bananas are not green”; both are okay.

Omitting the bracketing that tells the order of operations is confusing and grammatically incorrect. That costs 2 points.

- (6) (15 points) (Sect. 4.2 and 2.3) Prove by induction that  $\sum_{i=1}^n i^3 = \frac{n^2(n+1)^2}{4}$ .

Your proof should meet the standards for an induction proof as presented in class.

**Solution.** (Induction is expected for passing the class. You will see it again.)

First, the *induction statement*  $P(n)$  is the statement:  $\sum_{i=1}^n i^3 = \frac{n^2(n+1)^2}{4}$ .

*Base case.* We want to prove  $P(1)$ . (Note: I did not say to prove this statement for all  $n \geq 1$ , but that seems obvious.)

First, evaluate the left side:  $\sum_{i=1}^1 i^3 = 1^3$  by the definition of summations, and this = 1 by the definition of powers (you could omit the details about powers).

Next, evaluate the right side:  $\frac{1^2(1+1)^2}{4} = 1$ .

Finally, compare: They are equal. Therefore,  $P(1)$  is proved.

*Induction step.* Let  $n \geq 1$ . We assume  $P(n)$  and we want to deduce  $P(n+1)$ .

The assumption  $P(n)$  is that  $\sum_{i=1}^n i^3 = \frac{n^2(n+1)^2}{4}$ .

The statement to be proved is that  $\sum_{i=1}^{n+1} i^3 = \frac{(n+1)^2(n+2)^2}{4}$ .

We have

$$\begin{aligned} \sum_{i=1}^{n+1} i^3 &= \sum_{i=1}^n i^3 + (n+1)^3 && \text{by the definition of summation} \\ &= \frac{n^2(n+1)^2}{4} + (n+1)^3 && \text{by the induction assumption } P(n) \\ &= \frac{(n+1)^2(n+2)^2}{4} && \text{by algebra (I omit the details).} \end{aligned}$$

This proves  $P(n+1)$ , concluding the induction step.

By the Principle of Mathematical Induction,  $P(n)$  is proved for all  $n \geq 1$ . (It's important to state the range of  $n$  for which you have proved  $P(n)$ .)

- (7) (20 = 3+7+6+4 points) (Sect. 3.1–3, 5.1–2)  $A$  and  $B$  are subsets of the universe  $X$ .

(a) Formulate in logical form, using the definitions of set equality and containment, with any necessary quantifiers ( $\forall$ ,  $\exists$ ) and logical terms (and, or, not,  $\implies$ ,  $\iff$ ), the following statement:  $(A^c)^c = A$ . (Don't prove it.)

**Solution.**  $(\forall a)[(\text{NOT}[\text{NOT}(a \in A)]) \implies (a \in A)]$ .

or simply  $(\text{NOT}[\text{NOT}(a \in A)]) \implies (a \in A)$ .

Explanation: For any set  $S$ ,  $a \in S^c$  means (\*)  $a \notin S$ , i.e., NOT  $(a \in S)$ . For  $S = A^c$ , this becomes (1) NOT  $(a \in A^c)$ . We can also use (\*) to convert  $a \in A^c$  to (2) NOT  $(a \in A)$ . Substitute (2) into (1) and you get the answer.

- (b) Prove that  $A \subseteq B \implies B^c \subseteq A^c$ .

**Solution.** We want to prove that the assumption  $A \subseteq B$  implies the conclusion  $B^c \subseteq A^c$ .

Proof. Assume  $A \subseteq B$ . That means  $x \in A \implies x \in B$  (definition of set containment). The contrapositive is  $x \notin B \implies x \notin A$ . This means  $x \in B^c \implies x \in A^c$  (definition of complement). That means  $B^c \subseteq A^c$  (definition of set containment).

- (c) State the (A) converse, (B) contrapositive, and (C) inverse of the statement in part (7b).

**Solution.** (A)  $B^c \subseteq A^c \implies A \subseteq B$ .

(B)  $B^c \not\subseteq A^c \implies A \not\subseteq B$ .

(C)  $A \not\subseteq B \implies B^c \not\subseteq A^c$ .

N.B. You are expected to know these terms by heart.

- (d) Use the facts stated in parts (7a) and (7b) to prove the converse of (7b), without using any set-theory reasons.

**Solution.** In the formula of part (7b), replace  $A$  by  $B^c$  and  $B$  by  $A^c$ . This gives the statement  $B^c \subseteq A^c \implies (A^c)^c \subseteq (B^c)^c$ . This statement is true because  $A, B$  in the original formula were any sets.

Now use part (7a) to say that  $(A^c)^c = A$  and  $(B^c)^c = B$ . Thus, we have the formula  $B^c \subseteq A^c \implies A \subseteq B$ . QED

- (8) (5 points) (Sect. 6.3) In  $\mathbb{Z}_9$ :

- (a) Calculate  $[4] + [13]$  and  $[4] \cdot [7]$ . Express your answers in the form  $[s]$  where  $0 \leq s \leq 8$ .

**Solution.**  $[4] + [13] = [17] = [8]$ .  $[4] \cdot [7] = [28] = [1]$ .

- (b) Does  $[4]$  have a multiplicative inverse? If so, what is it?

**Solution.** Yes. By part (a)  $[4] \cdot [7] = [1]$  so  $[4]^{-1}$  exists and equals  $[7]$ .

- (9) (5 points) (Sect. 6.3) Find all integers  $x$  that satisfy the equation  $3x + 2 \equiv 0 \pmod{12}$ .

**Solution.** We want to find all  $x$  such that  $12 \mid ((3x + 2) - 0)$ . That is,  $3x + 2 = 12j$  for some integer  $j$ . Rearrange this:  $12j - 3x = 2$  for some integer  $j$ . Factor the left side:  $3(4j - x) = 2$  for some integer  $j$ . Oh, no!  $3 \nmid 2$  so this is impossible. Therefore, no  $x$  exists. (N.B. I made some kind of silly error in preparing this; the 2 should have been 3. But still it's a valid question.)

- (10) (15 points) (Sect. 6.1) Define the following relation on  $A =$  the set of integers  $\geq 0$ :  $m \sim n$  if  $m = n$  or  $mn = 6$ .

- (a) Prove this is an equivalence relation.

**Solution.** There is only one way to prove an equivalence relation: check the three properties.

*Reflexivity.* Is  $m \sim m$ ? That is, is  $m = m$  or  $m^2 = 6$ ? Yes, because  $m = m$ .

*Symmetry.* Suppose  $m \sim n$ . That is,  $m = n$  or  $mn = 6$ . Equivalently,  $n = m$  or  $nm = 6$ . That means  $n \sim m$ .

*Transitivity.* Suppose  $m \sim n$  and  $n \sim p$ . That means  $(m = n \text{ or } mn = 6)$  AND  $(n = p \text{ or } np = 6)$ . I think it's easiest to split this into cases.

Case 1:  $m = n$ . Then we know  $m \sim p$  by replacement of  $n$  by  $m$  in  $n \sim p$ .

Case 2:  $n = p$ . Then we know  $m \sim p$  by replacement of  $n$  by  $p$  in  $m \sim n$ .

Case 3:  $m \neq n$  and  $n \neq p$ . Then we know  $mn = 6$  and  $np = 6$ . Therefore,  $mn = np$ , so by commutativity and cancellation (*unless*  $n = 0$ ),  $m = p$ , hence  $m \sim p$ . But if  $n = 0$ , then  $mn = 0 \neq 6$ , so  $n$  cannot be 0. Thus, we have proved transitivity.

(b) Find the equivalence class of every integer  $n \in A$ .

**Solution.** Certainly,  $n \in [n]$ . Is there any other integer in  $[n]$ ? Yes,  $m \in [n]$  if  $mn = 6$ , so  $6/n \in [n]$  if  $6/n$  is an integer. That occurs if and only if  $n|6$ , i.e.,  $n = 1, 2, 3$ , or  $6$ . Thus, the equivalence classes for  $n \geq 0$  are

$[n] = \{n\}$  except that  $[1] = [6] = \{1, 6\}$  and  $[2] = [3] = \{2, 3\}$ .