

Math 300 C - Autumn 2024

Final Exam

December 9, 2024

Solutions

1. *By considering the situation modulo 7, show that there are infinitely many positive integers that are not expressible in the form $2^a + b^3$, where a and b are non-negative integers.*

Let a be a non-negative integer.

Then $a = 3m + r$ where $m, r \in \mathbb{Z}_{\geq 0}$ and $r = 0, 1$ or 2 .

Then $2^a = (2^3)^m 2^r \equiv (1)2^r \equiv 2^r \pmod{7}$.

Hence, $2^a \equiv 1, 2$, or $4 \pmod{7}$.

Every non-negative integer b is congruent to exactly one of $\{0, 1, 2, 3, 4, 5, 6\}$ modulo 7.

We create the following table of these values squared modulo 7:

b	b^3
0	0
1	1
2	$8 \equiv 1$
3	$27 \equiv 6$
4	$64 \equiv 1$
5	$5 \cdot 25 \equiv 5 \cdot 4 \equiv 6$
6	$6 \cdot 36 \equiv 6 \cdot 1 \equiv 6$

Hence, for any non-negative integer b , $b^3 \equiv 0, 1$ or $6 \pmod{7}$.

The following table shows all possible values of $2^a + b^3$ modulo 7 for $a, b \in \mathbb{Z}_{\geq 0}$:

$+$	1	2	4
0	1	2	4
1	2	3	5
6	0	1	3

Thus we see that $2^a + b^3 \not\equiv 6 \pmod{7}$ for any $a, b \in \mathbb{Z}_{\geq 0}$.

Since $7k + 6$ is congruent to 6 modulo 7 for all positive integers k , we conclude that there are infinitely many positive integers that are not expressible in the form $2^a + b^3$, where a and b are non-negative integers. ■

2. Let A, B and C be non-empty sets, and suppose $f : A \rightarrow C$ and $g : B \rightarrow C$.

Let $h = f \cup g$. Then $h \subseteq (A \cup B) \times C$.

Show that $h : A \cup B \rightarrow C$ iff $f(x) = g(x)$ for all $x \in A \cap B$.

Let A, B, C, f, g , and h be defined as above.

Suppose $f(x) = g(x)$ for all $x \in A \cap B$.

Suppose $x \in A \cup B$.

Suppose $x \in A$.

Then $(x, f(x)) \in f$, so $(x, f(x)) \in h$.

Suppose $x \in B$.

Then $(x, g(x)) \in g$, so $(x, g(x)) \in h$.

So, for all $x \in A \cup B$, there exists y in C such that $(x, y) \in h$.

Now, suppose there is an $x \in A \cup B$ and $y_1, y_2 \in C$, with $y_1 \neq y_2$ and $(x, y_1) \in h$ and $(x, y_2) \in h$.

If $x \in A$ and $x \notin B$, then this contradicts the assumption that f is a function.

If $x \in B$ and $x \notin A$, then this contradicts the assumption that g is a function.

If $x \in A \cap B$, then this contradicts the assumption that $f(x) = g(x)$ for all $x \in A \cap B$.

Hence, for all $x \in A \cup B$, there exists a unique $y \in C$ such that $(x, y) \in h$.

Thus, $h : A \cup B \rightarrow C$.

Suppose $h : A \cup B \rightarrow C$.

Suppose $x \in A \cap B$ and suppose $f(x) \neq g(x)$.

Then $(x, f(x)) \in h$ and $(x, g(x)) \in h$.

Hence, h is not a function from $A \cup B$, and this is a contradiction.

Thus $f(x) = g(x)$ for all $x \in A \cap B$. ■

3. Let

$$f : \mathbb{R} \rightarrow \mathcal{P}(\mathbb{R})$$

be defined by

$$f(x) = \{z \in \mathbb{R} : x + z \in \mathbb{Z}\}.$$

Show that f is not one-to-one and not onto.

First,

$$f(0) = \{z \in \mathbb{R} : z \in \mathbb{Z}\} = \mathbb{Z}$$

and

$$f(1) = \{z \in \mathbb{R} : z + 1 \in \mathbb{Z}\} = \mathbb{Z}$$

since every integer minus one is an integer, and if $z + 1$ is an integer, then $z + 1 - 1 = z$ is an integer.

Since $f(0) = f(1)$, f is not one to one.

Let $x \in \mathbb{R}$.

Then $-x \in f(x)$, since $x + (-x) = 0 \in \mathbb{Z}$.

Thus, $f(x)$ is never empty: it always contains $-x$.

Hence, there is no $x \in \mathbb{R}$ such that $f(x) = \emptyset$.

Since $\emptyset \in \mathcal{P}(\mathbb{R})$, we conclude that f is not onto.

4. (a) *Is the inverse of an equivalence relation necessarily an equivalence relation? Prove you are correct.*

Suppose R is an equivalence relation.

Suppose $(a, b) \in R^{-1}$.

Then $(b, a) \in R$, and, since R is symmetric, $(a, b) \in R$.

So $(a, b) \in R^{-1}$ implies $(a, b) \in R$, so $R^{-1} \subseteq R$.

Suppose $(a, b) \in R$.

Then, since R is symmetric, $(b, a) \in R$, and so $(a, b) \in R^{-1}$.

Hence, $(a, b) \in R$ implies $(a, b) \in R^{-1}$, so $R \subseteq R^{-1}$.

Thus, since $R \subseteq R^{-1}$ and $R^{-1} \subseteq R$,

$$R = R^{-1}.$$

Since R is an equivalence relation, R^{-1} is an equivalence relation. ■

- (b) *Give an example of an equivalence relation on the set $A = \{a, b, c\}$ that is not the identity function on A . You need not prove it is an equivalence relation.*

The set

$$\{(a, a), (b, b), (c, c), (a, b), (b, a)\}$$

is an equivalence relation and is not the identity function since it contains (a, b) with $a \neq b$.

5. Prove the following two theorems.

Let A and B be sets. Then:

(a) If $S \in \mathcal{P}(A \setminus B)$ and $S \neq \emptyset$, then $S \in \mathcal{P}(A) \setminus \mathcal{P}(B)$.

(b) $\mathcal{P}(A) \setminus \mathcal{P}(B)$ need not be a subset of $\mathcal{P}(A \setminus B)$.

Let A and B be sets.

(a) Suppose $S \in \mathcal{P}(A \setminus B)$, so $S \subseteq A \setminus B$.

Suppose $S \neq \emptyset$.

Let $x \in S$.

Then $x \in A \setminus B$, so $x \in A$ and $x \notin B$.

So, $x \in S$ implies $x \in A$, so $S \subseteq A$. Hence, $S \in \mathcal{P}(A)$.

Suppose $S \in \mathcal{P}(B)$.

Then $x \in S$ implies $x \in B$; this is a contradiction since $x \notin B$.

Hence, $S \notin \mathcal{P}(B)$.

Thus, $S \in \mathcal{P}(A) \setminus \mathcal{P}(B)$.

Thus, $S \in \mathcal{P}(A \setminus B)$ implies $S \in \mathcal{P}(A) \setminus \mathcal{P}(B)$.

Hence, $\mathcal{P}(A \setminus B) \subseteq \mathcal{P}(A) \setminus \mathcal{P}(B)$.

(b) Let $A = \{x, y\}$ and $B = \{y\}$.

Then

$$\mathcal{P}(A) = \{\emptyset, \{x\}, \{y\}, A\}$$

$$\mathcal{P}(B) = \{\emptyset, \{y\}\}$$

$$A \setminus B = \{x\}$$

$$\mathcal{P}(A \setminus B) = \{\emptyset, \{x\}\}$$

$$\mathcal{P}(A) \setminus \mathcal{P}(B) = \{\{x\}, A\}$$

Since $A \in \mathcal{P}(A) \setminus \mathcal{P}(B)$ but $A \notin \mathcal{P}(A \setminus B)$, we conclude that

$$\mathcal{P}(A) \setminus \mathcal{P}(B) \not\subseteq \mathcal{P}(A \setminus B).$$

Thus, for any sets A and B , $\mathcal{P}(A) \setminus \mathcal{P}(B)$ need not be a subset of $\mathcal{P}(A \setminus B)$. ■

6. Use induction to prove that, for all positive integers n ,

$$16 \mid 5^n + 12n - 1.$$

Proof:

For any $n \in \mathbb{Z}_{>0}$, let $P(n) = "16 \mid 5^n + 12n - 1"$.

Base case:

Let $n = 1$.

Then $5^n + 12n - 1 = 5 + 12 - 1 = 16$ so $16 \mid 5^n + 12n - 1$.

Hence, $P(1)$ is true.

Induction step:

Suppose $P(n)$ is true for some $n = k \in \mathbb{Z}_{>0}$.

So $16 \mid 5^k + 12k - 1$, and so there exists $m \in \mathbb{Z}_{>0}$ such that

$$5^k + 12k - 1 = 16m.$$

Then

$$\begin{aligned} 5^{k+1} + 12(k+1) - 1 &= 5(5^k + 12k - 1) - 5 \cdot 12k + 5 + 12(k+1) - 1 \\ &= 5(5^k + 12k - 1) - 48k + 16 \\ &= 5(16m) - 48k + 16 \\ &= 16(5m - 3k + 1). \end{aligned}$$

Since $5m - 3k + 1 \in \mathbb{Z}$, we conclude that $16 \mid 5^{k+1} + 12(k+1) - 1$, and hence $P(k+1)$ is true.

So, $P(k)$ implies $P(k+1)$ and hence, since $P(1)$ is true, by induction $P(n)$ is true for all $n \in \mathbb{Z}_{>0}$. ■

Elementary Properties of the Integers (EPIs)

Suppose a, b, c , and d are integers.

- **Closure:** $a + b$ and ab are integers.
- **Substitution of Equals:** If $a = b$, then $a + c = b + c$ and $ac = bc$.
- **Commutativity:** $a + b = b + a$ and $ab = ba$.
- **Associativity:** $(a + b) + c = a + (b + c)$ and $(ab)c = a(bc)$.
- **The Distributive Law:** $a(b + c) = ab + ac$
- **Identities:** $a + 0 = 0 + a = a$ and $a \cdot 1 = 1 \cdot a = a$.
 0 is called the additive identity.
 1 is called the multiplicative identity.
- **Additive Inverses:** There exists an integer $-a$ such that $a + (-a) = (-a) + a = 0$.
- **Trichotomy:** Exactly one of the following is true:
 $a > 0$, $-a > 0$, or $a = 0$.
- **The Well-Ordering Principle:** Every non-empty set of positive integers contains a smallest element.

1. $a \cdot 0 = 0$
2. If $a + c = b + c$, then $a = b$.
3. $-a = (-1) \cdot a$
4. $(-a) \cdot b = -(ab)$
5. $(-a) \cdot (-b) = ab$
6. If $ab = 0$, then $a = 0$ or $b = 0$.
7. If $a \leq b$ and $b \leq a$, then $a = b$.
8. If $a < b$ and $b < c$, then $a < c$.
9. If $a < b$, then $a + c < b + c$.
10. If $a < b$ and $0 < c$, then $ac < bc$.
11. If $a < b$ and $c < 0$, then $bc < ac$.
12. If $a < b$ and $c < d$, then $a + c < b + d$.
13. If $0 \leq a < b$ and $0 \leq c < d$, then $ac < bd$.
14. If $a < b$, then $-b < -a$.
15. $0 \leq a^2$, where $a^2 = a \cdot a$.
16. If $ab = 1$, then either $a = b = 1$ or $a = b = -1$.

Sets

$A \subseteq B$ iff $x \in A$ implies $x \in B$

$A = B$ iff $A \subseteq B$ and $B \subseteq A$

$x \in A \cup B$ iff $x \in A$ or $x \in B$

$x \in A \cap B$ iff $x \in A$ and $x \in B$

$x \in A \setminus B$ iff $x \in A$ and $x \notin B$

NOTE: Properties 8-14 hold if each $<$ is replaced with $\leq$.

Two theorems for reference:

Theorem DAS (Divisors are Smaller):

Let a and b be positive integers. Then $a|b$ implies $a \leq b$.

Euclid's Division Theorem:

Let m be a positive integer. For all $n \in \mathbb{Z}$, there exist integers k and r such that

$$n = mk + r$$

with $0 \leq r \leq m - 1$.