

Exam 3 Review

Chapters 4&5 (gcd problems only), 6, 7, 8, 9 and 10

Determine whether each proposition is true or false, and then prove or disprove it. Clearly indicate the method of proof.

1. Proposition. Given an integer a , then a is even if and only if $a^3 + 3a^2 + 5a$ is even.
2. Proposition. For every integer n , either $4|n^2$ or $4|(n^2 - 1)$.
3. Proposition. If a, b are integers, then $\gcd(a, b) \leq \gcd(5a, b^2)$.
4. Proposition. The number $\sqrt{7}$ is irrational.
5. Proposition. The number $\sqrt{15}$ is irrational.
6. Proposition. The set $A = \{a \in \mathbb{N}: a \text{ is prime} \wedge a \geq 100 \wedge a \leq 110\}$ has cardinality greater than 2.
7. Proposition. If A, B , and C are sets, then $(A \cup B) - C = (A - C) \cup (B - C)$.
8. Proposition. If A and B are sets, then $(A - B) \times B = (A \times B) - (B \times B)$.
9. Proposition. For $a, b \in \mathbb{R}$ with $b \neq 0$, if a irrational and ab is rational then b is irrational.
10. Proposition. If A and B are sets, then $P(A) - P(B) \subseteq P(A - B)$.
11. Proposition. If $x, y \in \mathbb{R}$ and $x^2 < y^2$ then $x < y$.
12. Proposition. Suppose $x, y \in \mathbb{R}$. Then $y^3 - yx = 2xy^2 - 2x^2$ if and only if $y = 2x$ or $y^2 = x$.
13. Proposition. For any integer $n \geq 0$, it follows that $9|(4^{3n} + 8)$.
14. Proposition. For any integer $n \geq 0$, it follows that $3|(n^3 + 5n + 6)$.

Exam 3 Review ANSWER KEY

If you discover an error please let me know, either in class, on the OpenLab, or by email to jreitz@citytech.cuny.edu. Corrections will be posted on the "Exam Reviews" page.

NOTE 1: For problems requiring you to prove something, there is usually more than one correct answer, and it is often possible to use more than one different type of proof (direct, contrapositive, or contradiction) correctly. The following are examples of correct solutions, yours may be different.

NOTE 2: As we have been working with proofs for several weeks, there are a few facts that we have used many times - for example the definitions of even and odd number - and which have become familiar and second-nature. You will notice that I will start moving away from stating explicitly when I employ these definitions, leaving it up to you to (mentally) fill in the justification when I say something like " n is even, so $n = 2a$ for some integer a ".

1. Proposition. Given an integer a , then a is even if and only if $a^3 + 3a^2 + 5a$ is even.

TRUE.

Proof. (Forward direction \Rightarrow , direct proof). Suppose a is even. Then $a = 2b$ for some integer b .

So $a^3 + 3a^2 + 5a = (2b)^2 + 3(2b)^2 + 5(2b) = 2(4b^3 + 6b^2 + 5b)$, which is even.

(Backward direction \Leftarrow , contrapositive proof). Suppose a is not even. Then a is odd, so

$a = 2b + 1$ for some integer b . So

$a^3 + 3a^2 + 5a = (2b + 1)^3 + 3(2b + 1)^2 + 5(2b + 1) = 2(4b^3 + 12b^2 + 14b + 4) + 1$, which is odd. \square

2. Proposition. For every integer n , either $4|n^2$ or $4|(n^2 - 1)$.

TRUE.

Proof. (Direct proof). Suppose n is an integer. Then n is either even or odd.

Case 1. Suppose n is even. Then $n = 2a$ for some integer a , and so $n^2 = (2a)^2 = 4a^2$. Thus $4|n^2$.

Case 2. Suppose n is odd. Then $n = 2a + 1$ for an integer a , and

$n^2 = (2a + 1)^2 = 4a^2 + 4a + 1$. Subtracting one from both sides, we see that

$n^2 - 1 = 4(a^2 + a)$, and so $4|(n^2 - 1)$. This completes the proof. \square

3. Proposition. If a, b are integers, then $\gcd(a, b) \leq \gcd(5a, b^2)$.

TRUE.

Proof. (Direct). Suppose that a, b are integers. Let $d = \gcd(a, b)$. Then $d|a$ and $d|b$, as d is a common divisor. Thus $a = dm$ and $b = dn$ where m, n are integers, by the definition of divides.

Since $a = dm$ we have $5a = 5dm$, and so $5a = d \cdot (5m)$. Thus $d|5a$. Similarly, $b = dn$

gives $b^2 = (dn)^2$, so $b^2 = d \cdot (dn^2)$. Thus $d|b^2$. We have now shown that d is a common

divisor of $5a$ and b^2 , so d is less than or equal to the greatest common divisor, $d \leq \gcd(5a, b^2)$,

and so we have $\gcd(a, b) \leq \gcd(5a, b^2)$. QED.

4. Proposition. The number $\sqrt{7}$ is irrational.

TRUE.

Proof. (Proof by contradiction). Suppose that $\sqrt{7}$ is rational. Then $\sqrt{7} = \frac{a}{b}$ for some integers a and b with no common factors. It follows that $7 = \frac{a^2}{b^2}$ and so $7b^2 = a^2$. Thus 7 divides a^2 , and by Euclid's Lemma it follows that 7 divides a , giving $a = 7k$ for some integer k . Substituting, we have $7b^2 = (7k)^2 = 49k^2$, and dividing by 7 we get $b^2 = 7k^2$. We have shown that 7 divides b^2 and by Euclid's Lemma, we see that 7 divides b . This contradicts the assumption that a and b have no common factors. \square

5. Proposition. The number $\sqrt{15}$ is irrational.

TRUE.

Proof. (Proof by contradiction). Suppose that $\sqrt{15}$ is rational. Then $\sqrt{15} = \frac{a}{b}$ for some integers a and b with no common factors. It follows that $15 = \frac{a^2}{b^2}$ and so $15b^2 = a^2$ and $3(5b^2) = a^2$.

Thus 3 divides a^2 , and by Euclid's Lemma it follows that 3 divides a , giving $a = 3k$ for some integer k . Substituting, we have $15b^2 = (3k)^2 = 9k^2$, and dividing by 3 we get $5b^2 = 3k^2$. We have shown that 3 divides $5b^2$ and, applying Euclid's Lemma twice, we see that 3 divides b . This contradicts the assumption that a and b have no common factors. \square

6. The set $A = \{a \in \mathbb{N} : a \text{ is prime} \wedge a \geq 100 \wedge a \leq 110\}$ has cardinality greater than 2.

TRUE.

Proof. (Proof by example!) The numbers 101, 103, 107 and 109 are all primes between 100 and 110. Thus they are all members of A , and so A has cardinality greater than 2. \square

7. Proposition. If A , B , and C are sets, then $(A \cup B) - C = (A - C) \cup (B - C)$.

TRUE.

Proof. (Forward direction, \subseteq , direct proof). Suppose $a \in (A \cup B) - C$. Then a is a member of A or B , but $a \notin C$. If $a \in A$ then $a \in (A - C)$, and if $a \in B$ then $a \in (B - C)$. In either case, we have $a \in (A - C) \cup (B - C)$. Therefore $(A \cup B) - C \subseteq (A - C) \cup (B - C)$ (Backward direction, \supseteq , direct proof). Conversely, suppose $a \in (A - C) \cup (B - C)$. Then a is either in $(A - C)$ or in $(B - C)$. If $a \in (A - C)$ then $a \in A$ and $a \notin C$, and if $a \in (B - C)$ then $a \in B$ and $a \notin C$. In either case, $a \notin C$, and so we have shown that a is a member of either A or B , but $a \notin C$. Thus $a \in (A \cup B) - C$, and so $(A \cup B) - C \supseteq (A - C) \cup (B - C)$.

Therefore $(A \cup B) - C = (A - C) \cup (B - C)$. \square

8. Proposition. If A and B are sets, then $(A - B) \times B = (A \times B) - (B \times B)$.

TRUE.

Proof. (Forward direction, \subseteq , direct proof). Suppose $(a, b) \in (A - B) \times B$. Then $a \in A$, $a \notin B$ and $b \in B$. Since $a \in A$ and $b \in B$, we have $(a, b) \in (A \times B)$, and since $a \notin B$ we have $(a, b) \notin (B \times B)$. Thus $(a, b) \in (A \times B) - (B \times B)$, and so $(A - B) \times B \subseteq (A \times B) - (B \times B)$

(Backward direction, \supseteq , direct proof). Conversely, suppose $(a, b) \in (A \times B) - (B \times B)$.

From $(a, b) \in (A \times B)$ we conclude that $a \in A$ and $b \in B$. Since $(a, b) \notin (B \times B)$ we must

have either $a \notin B$ or $b \notin B$, and since we have shown that $b \in B$ it follows that $a \notin B$. Thus $a \in (A - B)$, and so $(a, b) \in (A - B) \times B$. This shows that $(A - B) \times B \supseteq (A \times B) - (B \times B)$

Therefore $(A - B) \times B = (A \times B) - (B \times B)$. \square

9. Proposition. If a irrational and ab is rational then b is irrational.

TRUE.

Proof. (Proof by contradiction). Suppose that a is irrational and ab is rational, and b is rational.

Then $ab = \frac{p}{q}$ and $b = \frac{r}{s}$ where $p, q, r, s \in \mathbb{Z}$ and q, s are not zero (by the definition of rational), and so $\frac{p}{q} = ab = a \cdot \frac{r}{s}$. Thus $\frac{p}{q} = a \cdot \frac{r}{s}$, so solving for a give $a = \frac{ps}{qr}$. Since ps and qr are integers, it follows that a is rational, which contradicts our assumption that a is irrational. \square

10. Proposition. If A and B are sets, then $P(A) - P(B) \subseteq P(A - B)$.

FALSE.

Disproof. (Counterexample) Consider the sets $A = \{1, 2\}$ and $B = \{1\}$. The set $\{1, 2\}$ is a subset of A but not a subset of B , and so it is in $P(A) - P(B)$. However, it is not a subset of $A - B = \{2\}$, and so it is not in $P(A - B)$. \square

11. Proposition. If $x, y \in \mathbb{R}$ and $x^2 < y^2$ then $x < y$.

FALSE.

Disproof. (Counterexample) Suppose $x = 1$ and $y = -2$. Then $x^2 < y^2$ since $1 < 4$, but $x > y$. \square

12. Proposition. Suppose $x, y \in \mathbb{R}$. Then $y^3 - yx = 2xy^2 - 2x^2$ if and only if $y = 2x$ or $y^2 = x$.

TRUE.

Proof. (Forward direction, direct proof). Suppose $y^3 - yx = 2xy^2 - 2x^2$. Moving all terms to the left and factoring, we see that $(y^2 - x)(y - 2x) = 0$. By the zero product property, we must have $y^2 - x = 0$ or $y - 2x = 0$, and so $y = 2x$ or $y^2 = x$.

(Backwards direction, direct proof). Suppose $y = 2x$ or $y^2 = x$.

Case 1. $y = 2x$. Substituting, we see that the left side is

$$y^3 - yx = (2x)^3 - (2x)x = 8x^3 - 2x^2 \text{ and the right side is}$$

$$2xy^2 - 2x^2 = 2x(2x)^2 - 2x^2 = 8x^3 - 2x^2, \text{ and so the equation holds.}$$

Case 2. $y^2 = x$. Substituting again, we obtain on the left side $y^3 - yx = y^3 - y(y^2) = 0$, and

the on the right side $2xy^2 - 2x^2 = 2(y^2)y^2 - 2(y^2)^2 = 2y^4 - 2y^4 = 0$, and so the equation holds in this case as well. \square

13. Proposition. For any integer $n \geq 0$, it follows that $9 \mid (4^{3n} + 8)$.

TRUE

Proof. (Proof by induction)

Base step. If $n = 0$, then $4^{3 \cdot 0} + 8 = 9$, and we have $9 \mid 9$.

Inductive step. Assume $9 \mid 4^{3k} + 8$. Then $4^{3k} + 8 = 9a$ for some integer a . Multiplying both sides by $4^3 = 64$, we have:

$$4^3 \cdot 4^{3k} + 64 \cdot 8 = 64 \cdot 9a$$

$$4^{3k+3} + 512 = 576a$$

Subtracting 504 from both sides, we obtain

$$4^{3(k+1)} + 8 = 576a - 504$$

$$4^{3(k+1)} + 8 = 9(64a - 56)$$

and so $9|4^{3(k+1)} + 8$.

Thus by induction we have $\forall n \in \mathbb{N}, 9|(4^{3n} + 8)$. \square

14. Proposition. $\forall n \in \mathbb{N}$, it follows that $3|(n^3 + 5n + 6)$.

TRUE.

Proof. (Proof by induction).

Base step. If $n = 1$, then $1^3 + 5 \cdot 1 + 6 = 12$, and we have $3|12$.

Inductive step. Assume $3|(k^3 + 5k + 6)$. Then $k^3 + 5k + 6 = 3a$ for some integer a .

Adding $3k^2 + 3k + 6$ to both sides we obtain $k^3 + 3k^2 + 8k + 12 = 3a + 3k^2 + 3k + 6$.

Simplifying both sides, we see that $(k + 1)^3 + 5(k + 1) + 6 = 3(a + k^2 + k + 2)$ and, since the expression on the right in parentheses is an integer, we have

$3|((k + 1)^3 + 5(k + 1) + 6)$. Thus by induction we have $\forall n \in \mathbb{N}$, it follows that $3|(n^3 + 5n + 6)$. \square