Final Exam Review

For problems 1-8, determine whether each proposition is true or false, and then prove or disprove it. Clearly indicate the method of proof.

1. Proposition. If x is a natural number, then x is odd if and only if $x^2 - 4x + 3$ is even.
2. Proposition. If A, B, and C are sets, then $(A \cup B) \cap C = (A \cap C) \cup (B \cap C)$.
3. Proposition. $\forall n \in \mathbb{N}, n^2 - n + 41$ is prime.
4. Proposition. If $n \in \mathbb{N}$, then $1 \cdot 2 + 2 \cdot 3 + 3 \cdot 4 + 4 \cdot 5 + ... + n(n + 1) = \frac{n(n+1)(n+2)}{3}$.
5. Proposition. $\sqrt{12}$ is irrational.
6. Proposition. Let $a, b \in \mathbb{Z}, n \in \mathbb{N}$. If $a \equiv b (mod\, n)$ then $a^3 \equiv b^3 (mod\, n)$.
7. Proposition. For any integer $n \geq 0$, it follows that $9|(4^{3n} + 8)$.
8. Proposition. If A and B are sets, then $P(A - B) \subseteq P(A) - P(B)$.
9. Proposition. If m, n are integers, then $\gcd(m, n) \leq \gcd(m^3, n^3)$.

10. a. List the elements of the set: $\{x^2 : x \in \mathbb{Z}, |2x + 1| < 11\}$
    b. Find the cardinality of the set: $|\{\emptyset,\ 5,\ \pi,\ \{\emptyset\}, \{\{\emptyset\}\},\ \{\emptyset, 1, \{\emptyset\}\}\}|$
    c. Given the set $D = \{0, 1, 2, \emptyset\}$, answer True or False (and explain):
       i. $\{\emptyset\} \in D$ ii. $\{\emptyset, 2\} \subseteq D$ iii. $\{(2, 0),\ (\emptyset, \emptyset)\} \subseteq D \times D$
    d. Draw a Venn diagram for $(A \cap B) \cup (A \cap C)$
11. Given sets $A = \{a, b, c\}$, $B = \{b, c, d\}$ and $C = \{a, b, e\}$, and universal set $U = \{a, b, c, d, e, f\}$, find each of the following sets and state the cardinality:
    a. $(A \cup B) - (B \cap C)$ b. $P(B - C)$ c. $B \times C$ d. $\overline{A \cap C}$
12. a. Let $A_1 = \{-1, 2\}$, $A_2 = \{-3, 4\}$, $A_3 = \{-5, 6\}$ and in general for each $n \in \mathbb{N}$, $A_n = \{-2n + 1, 2n\}$. Find $\bigcup_{i=1}^{\infty} A_i$ and $\bigcap_{i=1}^{\infty} A_i$.
    b. Let $\mathbb{R}^+$ be the set of positive real numbers. For each $\alpha \in \mathbb{R}^+$, let A_α be the closed interval $[0, \alpha]$. Find $\bigcup_{\alpha \in \mathbb{R}^+} A_\alpha$ and $\bigcap_{\alpha \in \mathbb{R}^+} A_\alpha$.
13. a. Write a truth table: a. $P \wedge \sim (Q \Rightarrow R)$
    b. Determine whether the following two statements are logically equivalent by comparing rows in a truth table: $P \vee \sim Q$ and $\sim (P \Rightarrow Q)$
14. Translate each statement into English and decide whether it is true or false. Then find the negation of the statement, in both English and in symbols, and decide whether it is true or false.
    a. $\forall x \in \mathbb{R},\ (x \notin \mathbb{N} \Rightarrow x \notin \mathbb{Z})$
    b. $\exists n \in \mathbb{N},\ \forall m \in \mathbb{N},\ (nm \in E)$ *(where E is the set of even numbers)*
    c. $\forall a \in \mathbb{Z},\ (3|a \ \wedge\ 5|a) \vee \sim (15|a)$
15. Given the set $\{A, B, C, D, E, F, G, H, I, J\}$,

a. how many 4-element lists are possible if repetition is not allowed, and the first two elements must be vowels?

b. how many 5-element lists are possible if repetition is allowed, and the list must contain at least one repeated letter?

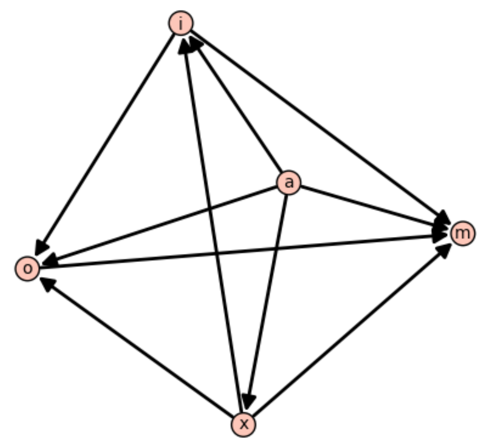
c. how many 6-element subsets are there?

d. how many ways are there of rearranging these letters if vowels must be kept together, and consonants must be kept together?

16. a. The relation R on the set A is represented by the graph at right. Identify the sets A and R. Determine whether R is reflexive, symmetric, transitive, antisymmetric or irreflexive (explain why in each case).

b. Consider the relation S = { (3,3), (4,4), (4,5), (5,4), (5,5), (6,6), (6,7), (7,6), (7,7), (8,8)} on the set $B = \{3, 4, 5, 6, 7, 8\}$. Sketch a graph representing S. Is S an equivalence relation (justify your answer)? If so, list the equivalence classes.

c. Prove that the relation R on $\mathbb{Z}$ given by xRy if and only if $x \equiv y \ mod\ 5$is an equivalence relation, and describe its equivalence classes.



17. a. Suppose $n \in \mathbb{N}$. Prove that addition for $\mathbb{Z}_n$ is well-defined.

b. Suppose $n \in \mathbb{N}$. Prove that multiplication for $\mathbb{Z}_n$ is well-defined.

Final Exam 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.

NOTE: 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.

1. Proposition. If *x* is a natural number, then *x* is odd if and only if $x^2 - 4x + 3$ is even.
   TRUE.
   Proof. (Forward direction ⇒, direct proof). Suppose *x* is odd. Then $x = 2b + 1$ for some integer *b*. So $x^2 - 4x + 3 = (2b + 1)^2 - 4(2b + 1) + 3 = 4b^2 - 4b = 2(2b^2 - 2b)$, which is even.
   (Backward direction ⇐, contrapositive proof). Suppose *x* is even. Then $x = 2b$ for some integer *b*. So $x^2 - 4x + 3 = (2b)^2 - 4(2b) + 3 = 4b^2 - 8b + 3 = 2(2b^2 - 4b + 1) + 1$, which is odd. ☐
2. Proposition. If *A, B,* and *C* are sets, then $(A \cup B) \cap C = (A \cap C) \cup (B \cap C)$.
   Proof. (Forward direction, ⊆, direct proof). Suppose $a \in (A \cup B) \cap C$. Then $a \in C$, and either $a \in A$ or $a \in B$. Thus there are two cases:
   Case 1: if $a \in A$, then $a \in A \cap C$, and
   Case 2: if $a \in B$, then $a \in B \cap C$.
   In either case, it follows that $a \in (A \cap C) \cup (B \cap C)$.
   (Backward direction, ⊇, direct proof). Conversely, suppose $a \in (A \cap C) \cup (B \cap C)$. Then either $a \in A \cap C$ or $a \in (B \cap C)$. It follows that *a* is either in *A* or in *B*, and in both cases we therefore have $a \in A \cup B$. Since $a \in C$, it follows that $a \in (A \cup B) \cap C$.☐
3. Proposition. $\forall n \in \mathbb{N}$, $n^2 - n + 41$ is prime.
   The proposition is false.
   Disproof. If *n=41*, then $n^2 - n + 41 = 1681 = 41^2$, which is not prime. ☐
4. Proposition. If $n \in \mathbb{N}$, then $1 \cdot 2 + 2 \cdot 3 + 3 \cdot 4 + 4 \cdot 5 + ... + n(n + 1) = \frac{n(n+1)(n+2)}{3}$.
   Proof. (Proof by induction).
   Base step. If $n = 1$, the expression *P(1)* gives $1 \cdot 2 = \frac{1(2)(3)}{3}$, or $2 = 2$.
   Inductive step. Suppose *P(k)* holds for some natural number *k*, that is
   $1 \cdot 2 + 2 \cdot 3 + 3 \cdot 4 + 4 \cdot 5 + ... + k(k + 1) = \frac{k(k+1)(k+2)}{3}$. Adding $(k + 1)(k + 2)$ to both sides, we obtain
   $1 \cdot 2 + 2 \cdot 3 + 3 \cdot 4 + 4 \cdot 5 + ... + k(k + 1) + (k + 1)(k + 2) = \frac{k(k+1)(k+2)}{3} + (k + 1)(k + 2)$
   . Note that the left side equals the left side of *P(k+1)*. Simplifying the right side gives
   $\frac{k(k+1)(k+2)}{3} + (k + 1)(k + 2) = \frac{k(k+1)(k+2)}{3} + \frac{3(k+1)(k+2)}{3} = \frac{(k+1)(k+2)(k+3)}{3}$, which is the right side of *P(k+1)*, and so we have prove *P(k+1)*.

It follows by induction that for all $n \in \mathbb{N}$,
$1 \cdot 2 + 2 \cdot 3 + 3 \cdot 4 + 4 \cdot 5 + ... + n(n + 1) = \frac{n(n+1)(n+2)}{3}$.

5. Proposition. $\sqrt{12}$ is irrational.
Proof. (Proof by contradiction) Suppose $\sqrt{12}$ is rational. Then $\sqrt{12} = \frac{a}{b}$ for some integers *a,b*, by the definition of rational number, and we can assume WLOG that *a* and *b* have no common factors. Then $12 = \frac{a^2}{b^2}$, so $12b^2 = a^2$, and so $a^2 = 3 \cdot 4b^2$. As $4b^2$ is an integer, this shows that a^2 is divisible by 3. It follows by Euclid's Lemma that *a* is divisible by 3, and so $a = 3c$ for some integer *c*. Substituting into $12b^2 = a^2$ we have $12b^2 = (3c)^2$, so $12b^2 = 9c^2$, and $4b^2 = 3c^2$. Therefore $4b^2$ is divisible by 3. Applying Euclid's Lemma, we see that 3 must divide either 4 or b^2, and as 3 does not divide 4 it follows that $3|b^2$. Applying Euclid's Lemma once again we see that 3 divides *b*, and so *a* and *b* have a common factor of 3. This contradicts our assumption that *a* and *b* have no common factors. ☐
NOTE: The statement C for which we proved $C \wedge \sim C$ is
C: a and b have no common factors.

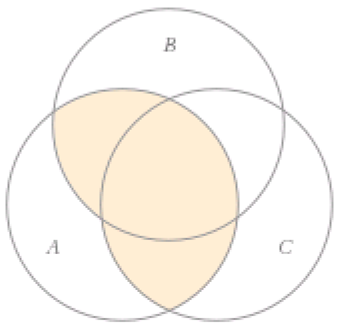
6. Proposition. Let $a, b \in \mathbb{Z}, n \in \mathbb{N}$. If $a \equiv b (mod\, n)$ then $a^3 \equiv b^3 (mod\, n)$.
Proof. (Direct proof). Suppose $a \equiv b(mod\, n)$. Then $n|(a - b)$, and so $a - b = nk$for some integer *k*. Taking the third power of both sides yields $(a - b)^3 = (nk)^3$, so
$a^3 - 3a^2b + 3ab^2 - b^3 = n^3k^3$, and $a^3 - b^3 = n^3k^3 + 3a^2b - 3ab^2$. Factoring the last two terms gives $a^3 - b^3 = n^3k^3 + 3ab(a - b)$, and substituting $a - b = nk$ gives
$a^3 - b^3 = n^3k^3 + 3abnk = n(n^2k^3 + 3abk)$. This shows that $n|a^3 - b^3$, so $a^3 \equiv b^3 (mod\, n)$.
☐

7. Proposition. For any integer $n \geq 0$, it follows that $9|(4^{3n} + 8)$.
TRUE
Proof. (Proof by induction)
Base step. If $n = 0$, then $4^{3 \cdot 0} + 8 = 9$, and we have $9|9$.
Inductive step. Assume $9|4^{3k} + 8$. 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 $\forall n \in \mathbb{N}, 9|(4^{3n} + 8)$.☐

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

Disproof. (Direct proof). Consider the empty set $\emptyset$. Note that the empty set is a subset of every set, so $\emptyset \in P(A - B)$. Also $\emptyset \in P(A)$, but since $\emptyset \in P(B)$ we have that $\emptyset \notin P(A) - P(B)$. So the left side contains the element $\emptyset$but the right side does not, so the left side is not a subset of the right side. ☐

9. Proposition. If m, n are integers, then $\gcd(m, n) \leq \gcd(m^3, n^3)$.
Proof. (Direct proof). Suppose m,n are integers. Let $d = \gcd(m, n)$. Then d is a common divisor of m and n, so $d|m$ and $d|n$. Thus $m = da$ and $n = db$ for some integers a and b, by definition of divides. Since $m = da$, we have $m^3 = (da)^3$ and so $m^3 = d(d^2a^3)$. Thus $d|m^3$. Similarly we can show that $d\ |n^3$, and so d is a common divisor of m^3 and n^3. Thus $d \leq \gcd(m^3,\ n^3)$, and so $\gcd(m, n) \leq \gcd(m^3, n^3)$.☐
10. a. {0, 1, 4, 9, 16, 25} b. 6 c. i. F ii. T iii. T
d.



11. a. {a, c, d} b. { $\emptyset$, $\{c\}$, $\{d\}$, $\{c, d\}$ } c. { (b,a), (b,b,), (b,e), (c,a), (c,b), (c,e), (d,a), (d,b), (d,e) } d. {c,d,e,f}
12. a. $\bigcup_{i=1}^{\infty} A_i = \{... -5,\ -3,\ -1,\ 2,\ 4,\ 6,\ 8,\ ...\}$ *(that is, the positive even integers and the negative odd integers)*. $\bigcap_{i=1}^{\infty} A_i = \emptyset$.

b. $\bigcup_{\alpha\in\mathbb{R}^+} A_\alpha = [0, \infty)$ and $\bigcap_{\alpha\in\mathbb{R}^+} A_\alpha = \{0\}$.
13. a.

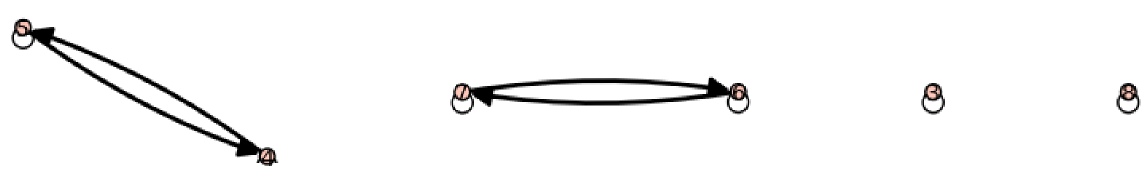
P	Q	R	$Q \Rightarrow R$	$\sim (Q \Rightarrow R)$	$P \wedge\sim (Q \Rightarrow R)$
T	T	T	T	F	F
T	T	F	F	T	T
T	F	T	T	F	F
T	F	F	T	F	F
F	T	T	T	F	F

F	T	F	F	T	F
F	F	T	T	F	F
F	F	F	T	F	F

b. They are not logically equivalent.

P	Q	$P \vee \sim Q$	$\sim (P \Rightarrow Q)$
T	T	T	F
T	F	T	T
F	T	F	F
F	F	T	F

14. a. In english, "For every real number x, if x is not a natural number then x is not an integer." FALSE (for example, x=-1 is not a natural number, but it is an integer).
Negation: $\exists x \in \mathbb{R}, (x \notin \mathbb{N} \wedge x \in \mathbb{Z})$. "There is a real number x such that x is not a natural number but x is an integer." TRUE
b. In english, "There is a natural number *n* such that for every natural number *m*, the product *nm* is an even number." TRUE, (for example n=2)
Negation: $\forall n \in \mathbb{N}, \exists m \in \mathbb{N}, (n \cdot m \notin E)$ "For every natural number *n* there is a natural number *m* such that the product *nm* is not even." FALSE
c. "For every integer *a*, either 3 divides *a* and 5 divides *a*, or 15 does not divide *a*." TRUE.
Negation: $\exists a \in \mathbb{Z}, (\sim 3|a \ \vee \sim 5|a) \wedge (15|a)$ "There is an integer *a* such that either 3 does not divide a, or 5 does not divide a, and 15 divides a". FALSE (if either 3 or 5 does not divide *a*, the 15 cannot divide *a*)
15. a. $3 \cdot 2 \cdot 8 \cdot 7 = 336$ b. $10^5 - \frac{10!}{5!} = 69760$ c. $\binom{10}{6} = 210$ d. $2 \cdot 7! \cdot 3! = 60480$
16. a. R is not reflexive (no point is connected to itself).
R is not symmetric (for example aRi but not iRa).
R is transitive (for example aRi and iRm, and aRm).
R is antisymmetric (all arrows go only one direction).
R is irreflexive (no point is connected to itself).
b.



Yes, S is an equivalence relation (it is reflexive, symmetric, and transitive). There are four equivalence classes: {3}, {4,5}, {6,7}, {8}
c. *R* is reflexive: Note that $5|0$, so $5|(x - x)$, so $x \equiv x (mod 5)$. Therefore *R* is reflexive.
R is symmetric. Suppose $x \equiv y (mod\ 5)$. Then $5|(x - y)$, and so $x - y = 5n$ for some integer *n*. Multiplying by -1, we obtain $y - x = 5(-n)$, and so $5|(y - x)$. Thus

$y \equiv x(mod\,5)$, and so R is symmetric.
R is transitive. Suppose $x \equiv y(mod\,5)$ and $y \equiv z(mod\,5)$. It follows that $x - y = 5n$ and $y - z = 5m$ for some integers n and m. Adding equations, we get $x - z = 5(n + m)$, and so $5|(x - z)$. Thus $x \equiv z(mod\,5)$. Thus R is transitive.
It follows that R is an equivalence relation. It has 5 equivalence classes, [0], [1], [2], [3], [4], distinguished by their remainder when divided by 5.

17. a. Suppose $n \in \mathbb{N}$. Prove that addition for $\mathbb{Z}_n$ is well-defined.

Proof. Suppose a, a', b, b' are integers with $[a] = [a']$ and $[b] = [b']$. Then $a \equiv a'\,mod\,n$ and $b \equiv b'\,mod\,n$. By the definition of congruence, we have $n|a - a'$ and $n|b - b'$, and so $a - a' = nx$ and $b - b' = ny$ for some integers m,n. Adding the equations, we have $a - a' + b - b' = nx + ny$, so $(a + b) - (a' + b') = n(x + y)$. Thus $a + b \equiv a' + b'\,mod\,n$, and so $[a + b] = [a' + b']$. Thus adding two equivalence classes in $\mathbb{Z}_n$ gives the same results regardless of the representative of the class that is chosen, and so addition for $\mathbb{Z}_n$ is well-defined.☐

b. Suppose $n \in \mathbb{N}$. Prove that multiplication for $\mathbb{Z}_n$ is well-defined.

Proof. As above, suppose a, a', b, b' are integers with $[a] = [a']$ and $[b] = [b']$. Then $a \equiv a'\,mod\,n$ and $b \equiv b'\,mod\,n$. By the definition of congruence, we have $n|a - a'$ and $n|b - b'$, and so $a - a' = nx$ and $b - b' = ny$ for some integers m,n. Multiplying the equations, we have $(a - a') \cdot (b - b') = nx \cdot ny$, so $ab - a'b - ab' + a'b' = n(xny)$. Adding $a'b + ab' - 2a'b'$ to both sides, we obtain
$ab - a'b' = n(xny) + a'b + ab' - 2a'b'$. Grouping the right side yields
$ab - a'b' = n(xny) + a'b - a'b' + ab' - a'b'$, and factoring gives
$ab - a'b' = n(xny) + a'(b - b') + b'(a - a')$. Substituting for the expressions in parentheses, we find $ab - a'b' = n(xny) + a'(ny) + b'(nx)$, and factoring n on the right side gives $ab - a'b' = n(xny + a'y + b'x)$ Thus $ab \equiv a'b'\,mod\,n$, and so $[ab] = [a'b']$. Thus multiplying two equivalence classes in $\mathbb{Z}_n$ gives the same results regardless of the representative of the class that is chosen, and so multiplication for $\mathbb{Z}_n$ is well-defined.☐