MATH 2112/CSCI 2112, Discrete Structures I
Winter 2007
Toby Kenney
Make-up Midterm Examination
Model Solutions

Answer all questions.

1 *Which of the following are true when* $A = \{1, 3, 7\}$ *and* $B = \{0, 4, 6, 10, 12, 34\}$*? Justify your answers.*

(a) $(\exists x \in A)(\forall y \in B)(x + y$ *is prime*$)$

This is true. When $x = 7$ the values of $x + y$ are as follows:

y	$7 + y$
0	7
4	11
6	13
10	17
12	19
34	41

These are all prime.

(b) $(\forall x \in A)(\exists y \in B)(x + y$ *is prime*$)$

This is also true. The following choices for y all work:

x	y
1	4,6,10,12
3	0,4,10,34
7	0,4,6,10,12,34

2 *Use Euclid's algorithm to find the greatest common divisor of 193 and 114. Write down all the steps involved. Use your calculations to find integers a and b such that* $193a + 114b$ *is the greatest common divisor of 193 and 114.*

$$\begin{aligned} 193 &= 114 + 79 \\ 114 &= 79 + 35 \\ 79 &= 35 \times 2 + 9 \\ 35 &= 3 \times 9 + 8 \\ 9 &= 8 + 1 \\ 8 &= 8 \times 1 \end{aligned}$$

So the greatest common divisor is 1. Working backwards:

$$\begin{aligned}
1 &= 9 - 8 = 9 - (35 - 3 \times 9) = 4 \times 9 - 35 \\
&= 4 \times (79 - 2 \times 35) - 35 = 4 \times 79 - 9 \times 35 \\
&= 4 \times 79 - 9 \times (114 - 79) = 13 \times 79 - 9 \times 114 \\
&= 13 \times (193 - 114) - 9 \times 114 = 13 \times 193 - 22 \times 114
\end{aligned}$$

So $a = 13$, $b = -22$ works.

3 *Use universal instantiation and rules of inference to show that the following argument is valid.*

$$(\forall x)(x \in A \to (\neg(x \in B)))$$
$$(y \in A \vee y \in C) \wedge (\neg(y \in B) \to y \in C)$$
$$\therefore y \in C$$

$(\forall x)(x \in A \to (\neg(x \in B)))$	Premise
$y \in A \to (\neg(y \in B))$	Universal instantiation
$(y \in A \vee y \in C) \wedge (\neg(y \in B) \to y \in C)$	Premise
$\neg(y \in B) \to y \in C$	Specialisation
$y \in A \to y \in C$	Transitivity
$y \in A \vee y \in C$	Specialisation from line 3
$y \in C \to y \in C$	Tautology
$y \in C$	Division into cases

4 *Which of the following pairs of propositions are logically equivalent? Justify your answers.*

(a) $(p \vee q) \to r$ *and* $(p \to r) \vee (q \to r)$.

These are not logically equivalent – When p is true but q and r are both false, the first proposition is false, while the second one is true.

(b) $p \vee (\neg q \to r)$ *and* $q \vee (\neg p \to r)$.

The truth tables are:

p	q	r	$\neg q$	$\neg q \rightarrow r$	$p \vee (\neg q \rightarrow r)$
0	0	0	1	0	0
0	0	1	1	1	1
0	1	0	0	1	1
0	1	1	0	1	1
1	0	0	1	0	1
1	0	1	1	1	1
1	1	0	0	1	1
1	1	1	0	1	1

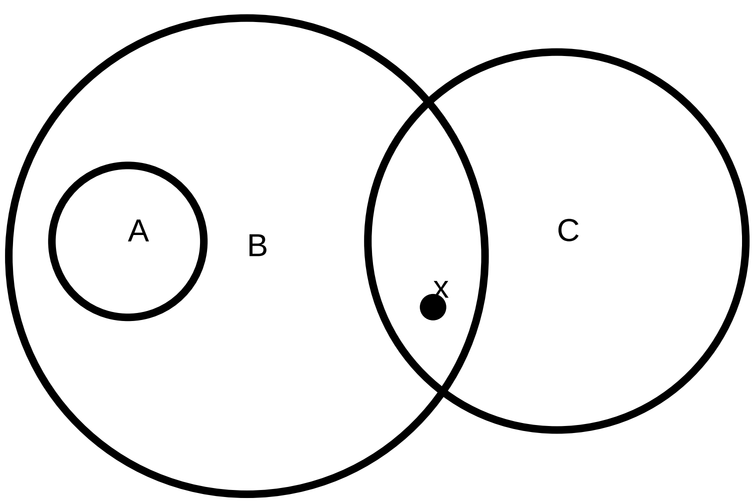
and

p	q	r	$\neg p$	$\neg p \rightarrow r$	$q \vee (\neg p \rightarrow r)$
0	0	0	1	0	0
0	0	1	1	1	1
0	1	0	1	0	1
0	1	1	1	1	1
1	0	0	0	1	1
1	0	1	0	1	1
1	1	0	0	1	1
1	1	1	0	1	1

The columns for $p \vee (\neg q \rightarrow r)$ and $q \vee (\neg p \rightarrow r)$ are the same. Therefore, they are logically equivalent.

5 *Use a Venn diagram to show the following argument is invalid:*

$$(\forall x \in A)(x \in B)$$
$$(\exists x \in B)(x \in C)$$
$$\therefore (\exists x \in A)(x \in C)$$



6 *Prove or disprove the following. You may use results proved in the course or the homework sheets, provided you state them clearly.*

(a) There are infinitely many primes congruent to either 2 or 3 modulo 5. [You may assume that any integer that is congruent to 2 or 3 modulo 5 is divisible by a prime number congruent to 2 or 3 modulo 5. You may also assume that if n is not divisible by 5, then $n^4 \equiv 1 \pmod 5$.]

This is true.

Proof. Suppose there are only finitely many such primes. Call them $p_1, p_2, \ldots, p_k$. Now consider $N = (p_1 p_2 \cdots p_k)^4 + 1$. N is congruent to 2 modulo 5, since $p_1 p_2 \cdots p_k$ is not divisible by 5, so $(p_1 p_2 \cdots p_k)^4 \equiv 1 \pmod 5$, so N has a prime factor congruent to 2 or 3 modulo 5. This prime factor can't be any of $p_1, p_2, \ldots, p_k$, since they all divide $N - 1$. Therefore, there must be a prime congruent to 2 or 3 modulo 5 that is not one of $p_1, p_2, \ldots, p_k$. This is a contradiction since we said that $p_1, p_2, \ldots, p_k$ were all such primes. Therefore, our assumption that there were only finitely many such primes must be false. Therefore, there must be infinitely many such primes. □

(b) $\sqrt[3]{16}$ *is irrational.*

This is true.

Proof. Suppose that $\sqrt[3]{16}$ is rational. Then it can be written as $\frac{a}{b}$ for $a, b \in \mathbb{Z}$, $b \neq 0$. Let $a' = \frac{a}{(a,b)}$ and $b' = \frac{b}{(a,b)}$. Then $(a', b') = 0$, since if $d|a'$ and $d|b'$, then $d(a,b)|a$ and $d(a,b)|b$, so $d(a,b) \leqslant (a,b)$, and therefore, $d \leqslant 1$. Also, $\frac{a'}{b'} = \sqrt[3]{16}$, and $b' \neq 0$.

Now, cubing the equation, we get:

$$\begin{aligned} \frac{a'^3}{b'^3} &= 16 \\ a'^3 &= 16b'^3 \end{aligned}$$

Therefore, $2|a'^3$, so by unique prime factorisation, $2|a'$. Therefore, there is some integer k such that $a' = 2k$. This gives $8k^3 = 16b'^3$. Therefore, $k^3 = 2b'^3$. Thus, $2|k$. Let $k = 2l$. Hence, $2b'^3 = 8l^3$. Therefore, $b'^3 = 4l^3$, so $2|b'^3$, and therefore, $2|b'$. This contradicts the fact that $(a', b') = 1$. Therefore, our assumption that $\sqrt[3]{16}$ was rational must be false, so it must be irrational. □

(c) There is a natural number n such that $2n^2 + 3n + 1$ is prime.

This is false.

Proof. $2n^2 + 3n + 1 = (2n + 1)(n + 1)$. If $n = 0$, then $2n^2 + 3n + 1 = 1$ which is not prime. If $n \geqslant 1$, then $n + 1$ and $2n + 1$ must both be greater than 1, so we have expressed $2n^2 + 3n + 1$ as a product of two integers that are both more than 1. Therefore, it is not prime. □

(d) There is a natural number n such that $n^2 + 4n - 6$ is prime.

This is true. When $n = 7$, $n^2 + 4n - 6 = 49 + 28 - 6 = 71$, which is prime.

(e) $2^{12} + 3^{26} + 5^{29}$ is divisible by 11.

This is false.

Proof. Calculate some powers of 2,3, and 5 modulo 11:

n	$2^n \pmod{11}$	$3^n \pmod{11}$	$5^n \pmod{11}$
2	4	9	3
4	5	4	9
5	10	1	1
10	1	1	1

We have that $2^{10} \equiv 1 \pmod{11}$, so $2^{12} \equiv 2^2 \equiv 4 \pmod{11}$. Similarly, $3^5 \equiv 1 \pmod{11}$, so $3^{26} \equiv 3^1 \equiv 3 \pmod{11}$. Finally, $5^5 \equiv 1 \pmod{11}$, so $5^2 9 \equiv 5^4 \equiv 9 \pmod{11}$. Therefore, $2^{12}+3^{26}+5^{29} \equiv 4+3+9 \equiv 5 \pmod{11}$. Therefore, it is not divisible by 11. □

(f) For all natural numbers n, $\frac{n^3+5n+6}{3} = 2^{n+1}$.

This is false. When $n = 4$, $\frac{n^3+5n+6}{3} = \frac{64+20+6}{3} = \frac{90}{3} = 30 \neq 2^{4+1} = 32$.

7 *Find an integer k, such that for all natural numbers n, $\sum_{i=1}^{n} \frac{i(i+1)(2i+1)}{6} = \frac{n(n+1)^2(n+2)}{k}$. Prove that the formula works for your value of k. [Hint: try to prove the result by induction. The proof will only work for one value of k.]*

The value of k is 12. So we have

$$\sum_{i=1}^{n} \frac{i(i+1)(2i+1)}{6} = \frac{n(n+1)^2(n+2)}{12}$$

Proof. Induction on n. Base case: when $n = 0$, the sum is empty, so is 0, and $\frac{n(n+1)^2(n+2)}{12}$ is also 0.

Now assume $\sum_{i=1}^{n} \frac{i(i+1)(2i+1)}{6} = \frac{n(n+1)^2(n+2)}{12}$. We want to prove that $\sum_{i=1}^{n+1} \frac{i(i+1)(2i+1)}{6} = \frac{(n+1)(n+2)^2(n+3)}{12}$.

$$\begin{aligned}
\sum_{i=1}^{n+1} \frac{i(i+1)(2i+1)}{6} &= \sum_{i=1}^{n} \frac{i(i+1)(2i+1)}{6} + \frac{(n+1)(n+2)(2n+3)}{6} \\
&= \frac{n(n+1)^2(n+2)}{12} + \frac{(n+1)(n+2)(2n+3)}{6} \\
&= \frac{(n+1)(n+2)}{12}(n(n+1) + 2(2n+3)) \\
&= \frac{(n+1)(n+2)}{12}(n^2 + 5n + 6) \\
&= \frac{(n+1)(n+2)^2(n+3)}{12}
\end{aligned}$$

So by induction, the formula works for all $n \in \mathbb{N}$. ☐

8 *Find* $0 \leqslant n < 840$ *satisfying all the following congruences:*

$$n \equiv 5 \pmod 8 \quad (1)$$
$$n \equiv 4 \pmod{15} \quad (2)$$
$$n \equiv 6 \pmod 7 \quad (3)$$

Consider the first two congruences: The first one gives $n = 5+8k$ for some $k \in \mathbb{Z}$. From the second, we have $5+8k \equiv 4 \pmod{15}$, or equivalently $8k \equiv -1 \pmod{15}$. Note that $8 \times 2 \equiv 1 \pmod{15}$, so $8 \times -2 \equiv -1 \pmod{15}$. Therefore, $5 + 8 \times 13 = 109$ satisfies the first two congruences.

We now need to solve:

$$n \equiv 109 \pmod{120} \quad (4)$$
$$n \equiv 6 \pmod 7 \quad (5)$$

The first congruence gives $n = 109 + 120l$. Substituting into the second congruence, we get $4 + l \equiv 6 \pmod 7$ ($109 \equiv 4 \pmod 7$ and $120 \equiv 1 \pmod 7$). This gives $l \equiv 2 \pmod 7$, so $n = 109 + 120 \times 2 = 349$ satisfies all three congruences.

9 *Find a boolean expression for the following logic circuit.*

$$\neg((p \vee \neg q) \vee (\neg p \wedge r))$$