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

Answer all questions.

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

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

$\neg((\exists y \in C)(\neg(y \in A)))$	Premise
$(\forall y \in C)(\neg\neg(y \in A))$	Logical equivalence
$z \in C$	Premise
$\neg\neg(z \in A)$	Universal instantiation
$z \in A$	Logical equivalence
$(\forall x \in A)(x \in B)$	Premise
$z \in B$	Universal instantiation

2 *Which of the following are true when* $A = \{0, 2, 5, 7\}$ *and* $B = \{2, 3, 5, 8, 9, 28\}$*? Justify your answers.*

(a) $(\forall x \in A)(\exists y \in B)(x \times y$ *is a perfect square*$)$

This is true. We can choose the following values of y for each values of x:

x	y
0	2,3,5,8,9,28
2	2,8
5	5
7	28

(b) $(\exists y \in B)(\forall x \in A)(x \times y$ *is a perfect square*$)$

This is false – there is no y in B that works for every x in A (note that no number occurs in all the rows of the table above). Given any choice for y, we can choose the following x to make the assertion false:

y	x
2	5,7
3	2,5,7
5	2,7
8	5,7
9	2,5,7
28	2,5

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

(a) $\sqrt[3]{4}$ *is irrational.*

This is true.

Proof. Suppose $\sqrt[3]{4}$ is rational. Then there are integers p and q with $q \neq 0$ and $(p,q) = 1$, such that $\sqrt[3]{4} = \frac{p}{q}$. Cubing both sides, we get $4 = \frac{p^3}{q^3}$ or $4q^3 = p^3$. Thus, $2|p^3$. Therefore, $2|p$ by unique prime factorisation, so there is an integer p' such that $p = 2p'$. Therefore, $4q^3 = 8p'^3$, so $q^3 = 2p'^3$. Thus, $2|q^3$, so $2|q$ by unique prime factorisation. Therefore, p and q have the common divisor 2, contradicting the fact that $(p,q) = 1$. Therefore, we can't find integers p and q with $\frac{p}{q} = \sqrt[3]{4}$, so $\sqrt[3]{4}$ is irrational. □

(b) There is a natural number n such that $6n^3 + 12n^2 + 15n + 21$ *is prime.*

This is false.

Proof. $6n^3 + 12n^2 + 15n + 21 = 3(2n^3 + 4n^2 + 5n + 7)$, so if it is prime, then $2n^3 + 4n^2 + 5n + 7$ must be 1 or -1. However, all its terms are non-negative (since n is non-negative, so it is at least 7, so it can never be 1. Therefore, $6n^3 - 15n^2 + 12n - 21$ is never prime for n a natural number. □

(c) There is a natural number n such that $n^2 + 8n + 6$ *is prime.*

This is true.

Proof. When $n = 5$, $n^2 + 8n + 6 = 25 + 40 + 6 = 71$, which is prime. □

(d) $n^3 + 5 = m^6 + 9$ *has no integer solutions [Hint: try modulo 7]*

This is true.

Proof. Third and sixth powers modulo 7 are shown in the following table:

n	$n^3 \pmod 7$	$n^6 \pmod 7$
0	0	0
1	1	1
2	1	1
3	6	1
4	1	1
5	6	1
6	6	1

So all cubes are congruent to 0, 1, or 6 modulo 7. Therefore, $n^3 + 5$ is always congruent to one of 4, 5, or 6 modulo 7. On the other hand, m^6 is always congruent to 0 or 1 modulo 7. Therefore, $m^6 + 9$ is always congruent to 2 or 3 modulo 7. Therefore, $n^3 + 5 \equiv m^6 + 9 \pmod 7$ has no solutions, so $n^3 + 5 = m^6 + 9$ can't have any integer solutions. □

(e) For all natural numbers n, $\sum_{i=1}^{n} \frac{i(i+1)}{2} = \frac{n(n+1)(n+2)}{6}$

This is true.

Proof. Induction on n. When $n = 0$, both sides are clearly 0. Now suppose that

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

We need to show that

$$\sum_{i=1}^{n+1} \frac{i(i+1)}{2} = \frac{(n+1)(n+2)(n+3)}{6}$$

However,

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

So by induction, the formula holds for all natural numbers n. □

(f) There are infinitely many primes congruent to 3 modulo 6.

This is false.

Proof. Let p be a prime number congruent to 3 modulo 6. This means that $6|p-3$. Therefore, by transitivity of divisibility, $3|p-3$. This means that $p - 3 = 3k$ for some integer k, so $p = 3(k+1)$. Therefore, since p is prime, $k+1$ must be 1, and therefore, $p=3$. Thus, there are only finitely many prime numbers congruent to 3 modulo 6 (in particular, there is only one such prime number). $\square$

(g) There are infinitely many prime numbers p such that there is an integer n for which $n^2 \equiv -1 \pmod{p}$. [Hint: Suppose the set of all such prime numbers is $p_1, \ldots, p_k$, and consider $(p_1 p_2 \cdots p_k)^2 + 1$.]

This is true.

Proof. Suppose there are only finitely many prime numbers with this property. Let them be $p_1, \ldots, p_k$. Consider $m = (p_1 \cdots p_k)^2 + 1$. m is divisible by a prime number p (by unique prime factorisation). p cannot be any of $p_1, \ldots, p_k$, since these all divide $m-1$. However, if we let $n = p_1 \cdots p_k$, then $n^2 \equiv -1 \pmod{p}$, so p is another prime for which there is an integer n such that $n^2 \equiv -1 \pmod{p}$, contradicting our assumption that $p_1, \ldots, p_k$ were the only such primes. This means that we can't list all such primes, so there must be infinitely many of them. $\square$

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

(a) $(p \wedge \neg q) \vee (\neg p \wedge q)$ and $(p \vee q) \wedge \neg(p \wedge q)$.

The truth tables are as follows:

p	q	$\neg p$	$\neg q$	$p \wedge \neg q$	$q \wedge \neg p$	$(p \wedge \neg q) \vee (\neg p \wedge q)$
0	0	1	1	0	0	0
0	1	1	0	0	1	1
1	0	0	1	1	0	1
1	1	0	0	0	0	0

p	q	$p \vee q$	$p \wedge q$	$\neg(p \wedge q)$	$(p \vee q) \wedge \neg(p \wedge q)$
0	0	0	0	1	0
0	1	1	0	1	1
1	0	1	0	1	1
1	1	1	1	0	0

We see that the columns for $(p \wedge \neg q) \vee (\neg p \wedge q)$ and $(p \vee q) \wedge \neg(p \wedge q)$ are the same, so they are logically equivalent.

(b) $p \vee \neg q$ and $\neg(\neg p \vee q)$.

When p is true and q is true, the first proposition is true, while the second one is false, so they are not logically equivalent.

5 Find $0 \leqslant n < 630$ satisfying all the following congruences:

$$
\begin{aligned}
n &\equiv 3 \pmod{7} && (1)\\
n &\equiv 8 \pmod{10} && (2)\\
n &\equiv 4 \pmod{9} && (3)
\end{aligned}
$$

For the first two congruences,

$$\begin{aligned} n &\equiv 3 \pmod 7 \\ n &\equiv 8 \pmod{10} \end{aligned}$$

we note that $3 \times 7 \equiv 1 \pmod{10}$, so $3 + 5 \times (3 \times 7) \equiv 8 \pmod{10}$, and therefore, $3 + 5 \times 3 \times 7 = 108$ satisfies $108 \equiv 3 \pmod 7$ and $108 \equiv 8 \pmod{10}$. Also, $108 \equiv 38 \pmod{70}$, so 38 also satisfies $38 \equiv 3 \pmod 7$ and $38 \equiv 8 \pmod{10}$. Now we just need to solve the congruences

$$\begin{aligned} n &\equiv 38 \pmod{70} \\ n &\equiv 4 \pmod 9 \end{aligned}$$

Again, we note that $70 \equiv 7 \pmod 9$, so $70 \times 4 \equiv 1 \pmod 9$. Therefore, $38 + (70 \times 4) \times 2 \equiv 4 \pmod 9$, so $n = 598$ satisfies all three congruences.

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

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

7 *Use Euclid's algorithm to find the greatest common divisor of the following pairs of numbers. Write down all the steps involved. Use your calculations to find integers a and b such that a times the first number plus b times the second number is their greatest common divisor.*

(a) 238 and 133

$$\begin{aligned} 238 &= 133 + 105 \\ 133 &= 105 + 28 \\ 105 &= 3 \times 28 + 21 \\ 28 &= 21 + 7 \\ 21 &= 3 \times 7 \end{aligned}$$

So the greatest common divisor is 7. Working backwards:

$$\begin{aligned} 7 &= 28 - 21 = 28 - (105 - 3 \times 28) = 4 \times 28 - 105 = 4 \times (133 - 105) - 105 \\ &= 4 \times 133 - 5 \times 105 = 4 \times 133 - 5 \times (238 - 133) = 9 \times 133 - 5 \times 238 \end{aligned}$$

So $a = -5$ and $b = 9$ works.

(b) 289 and 102

$$
\begin{aligned}
289 &= 2 \times 102 + 85 \\
102 &= 85 + 17 \\
85 &= 5 \times 17
\end{aligned}
$$

So the greatest common divisor is 17. Working backwards:

$$17 = 102 - 85 = 102 - (289 - 2 \times 102) = 3 \times 102 - 289$$

So $a = -1$, $b = 3$ works.