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

1 *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) 159 and 265

$$\begin{aligned} 265 &= 159 + 106 \\ 159 &= 106 + 53 \\ 106 &= 2 \times 53 \end{aligned}$$

Therefore, the greatest common divisor is 53. Working backwards:

$$53 = 159 - 106 = 159 - (265 - 159) = 2 \times 159 - 265$$

So $a = 2, b = -1$ works.

(b) 237 and 115

$$\begin{aligned} 237 &= 2 \times 115 + 7 \\ 115 &= 16 \times 7 + 3 \\ 7 &= 2 \times 3 + 1 \end{aligned}$$
$$3 = 3 \times 1$$

Therefore, the greatest common divisor is 1. Working backwards:

$$1 = 7 - 2 \times 3 = 7 - 2 \times (115 - 16 \times 7) = 33 \times 7 - 2 \times 115$$
$$= 33 \times (237 - 2 \times 115) - 2 \times 115 = 33 \times 237 - 68 \times 115$$

So $a = 33, b = -68$ works.

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

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

The truth tables are as follows:

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

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

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

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

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

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

3 *Find boolean expressions for the following logic circuits.*

(a) $(P \wedge Q) \vee (\neg Q \wedge R)$

(b) $(\neg P \wedge (Q \vee \neg R)) \vee R$

4 *Which of the following are true when* $A = \{0, 1, 3, 5\}$ *and* $B = \{1, 2, 4, 6\}$*? Justify your answers.*

(a) $(\forall x \in A)(x + 1 \in B)$

This is true. For $x = 0$, $1 \in B$; for $x = 1$, $2 \in B$; for $x = 3$, $4 \in B$; and for $x = 5$, $6 \in B$.

(b) $(\exists x \in A)(x + 2 \in B)$

This is true. Let $x = 0$. Then $x + 2 = 2 \in B$.

(c) $(\forall x \in A)(\exists y \in B)(x + y \text{ is even})$

This is true: we can make the following choices for y:

x	y	k such that $x+y=2k$
0	2,4,6	1,2,3
1	1	1
3	1	2
5	1	3

(d) $(\exists y \in B)(\forall x \in A)(x+y \textit{ is even})$

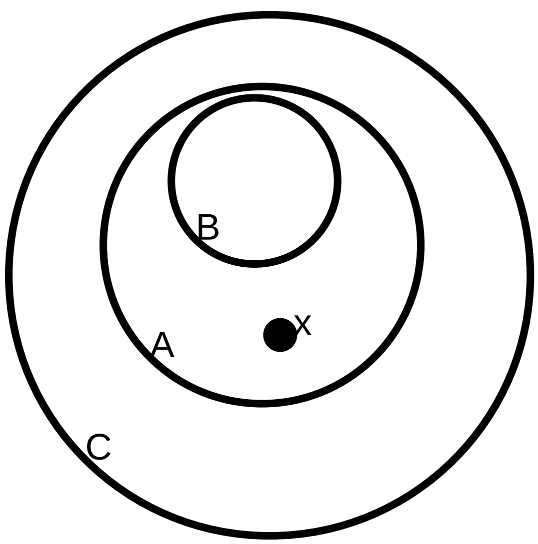
This is not true, since once y is chosen, we can choose x to make $x+y$ not even as follows:

y	x
1	0
2	1,3,5
4	1,3,5
6	1,3,5

5 *Use Venn diagrams to show the following arguments are invalid:*

(a)

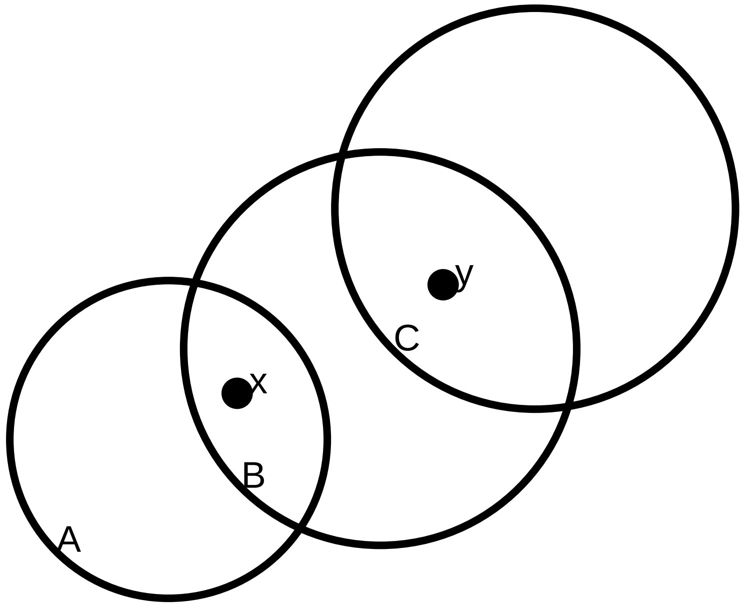
$$(\forall x \in A)(x \in B \vee x \in C)$$
$$(\forall x \in B)(x \in C)$$
$$\therefore (\forall x \in A)(x \in B)$$



(b)

$$(\exists x \in A)(x \in B)$$

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



6 *Use universal instantiation and rules of inference to show that the following arguments are valid.*

(a)

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

$(\forall x \in A)(x \in B \to x \in C)$	Premise
$y \in A \wedge y \in B$	Premise
$y \in A$	Specialisation
$y \in B \to y \in C$	Universal instantiation
$y \in B$	Specialisation
$y \in C$	Modus ponens

(b)

$$(\forall x \in A)(x \in B \vee \phi(x))$$
$$(\forall x \in A)(x \in C \vee \neg\phi(x))$$

$$y \in A \wedge \neg y \in C$$
$$\therefore y \in B$$

$(\forall x \in A)(x \in C \vee \neg\phi(x)$	Premise
$y \in A \wedge \neg y \in C$	Premise
$y \in A$	Specialisation
$y \in C \vee \neg\phi(y)$	Universal instantiation
$\neg y \in C$	Specialisation from line 2
$\neg\phi(y)$	Elimination
$(\forall x \in A)(x \in B \vee \phi(x))$	Premise
$y \in B \vee \phi(y)$	Universal instantiation
$y \in B$	Elimination

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

(a) $\sqrt[3]{7}$ *is rational.*

This is false.

Proof. Suppose $\sqrt[3]{7}$ were rational. Then it would be $\frac{a}{b}$ for integers a and b with $b \neq 0$. Now let $a' = \frac{a}{(a,b)}$ and $b' = \frac{b}{(a,b)}$. a' and b' are coprime, and $\frac{a'}{b'} = \sqrt[3]{7}$. We cube both sides to get $a'^3 = 7b'^3$. Thus $7|a'^3$, and so we must have $7|a'$ (see Sheet 4 Q.3). Therefore, $a' = 7c$ for some integer c. Hence, $(7c)^3 = 7b'^3$, and so $343c^3 = 7b'^3$, so $49c^3 = b^3$. Therefore, $7|b'$. This means that 7 is a common divisor of a' and b'. However, the greatest common divisor of a' and b' is 1. This is a contradiction, so our assumption that $\sqrt[3]{7}$ might be rational, must be false. Therefore, $\sqrt[3]{7}$ must be irrational □

(b) There is a natural number n *such that* $n^2 + 4n + 16$ *is prime.*

This is true.

Proof. When $n = 3$, $n^2 + 4n + 16 = 9 + 12 + 16 = 37$, which is prime. □

(c) There is a natural number n *such that* $n^2 - 169$ *is prime.*

This is false.

Proof. $n^2 - 169 = (n+13)(n-13)$. If neither $n+13$ nor $n-13$ is ± 1, then their product is either composite or 0, so it is not prime. Therefore, we only need to check the cases when $n - 13 = \pm 1$ ($n+13$ is never ± 1 for n a natural number, as $n+13 \geqslant 13$). These are $n = 12$ and $n = 14$. When $n = 12$, $n^2 - 169 = 144 - 169 = -25$, which is not prime. When $n = 14$, $n^2 - 169 = 196 - 169 = 27$, which is not prime. Therefore, $n^2 - 169$ is never prime. □

(d) All integers of the form $n^2 + n + 41$ are prime for $n \in \mathbb{N}$.

This is false.

Proof. When $n = 41$, $n^2 + n + 41 = 41^2 + 41 \times 2 = 41 \times 43$, which is not prime. (When $n = 40$, $n^2 + n + 41 = 40(40+1) + 41 = 41 \times 41$, which is also not prime.) □

(e) $2^{135} + 3^{98} + 5^{32}$ is divisible by 7.

This is true.

Proof. $2^3 = 8 \equiv 1 \pmod 7$. Therefore, for any natural number n, $2^{3n} \equiv 1^n \equiv 1 \pmod 7$. Hence, $2^{135} \equiv 1 \pmod 7$. Similarly, $3^2 = 9 \equiv 2 \pmod 7$. Therefore, for any natural number n, $3^{6n} \equiv 2^{3n} \equiv 1 \pmod 7$. Therefore, $3^{96} \equiv 1 \pmod 7$, so $3^{98} = 3^2 \times 3^{96} \equiv 3^2 \equiv 2 \pmod 7$. Finally, $5^2 = 25 \equiv 4 \pmod 7$, $5^3 \equiv 4 \times 5 \equiv 6 \pmod 7$, so $5^6 \equiv 6^2 \equiv 1 \pmod 7$. Therefore, $5^{30} \equiv 1^5 \equiv 1 \pmod 7$, so $5^{32} \equiv 5^2 \equiv 4 \pmod 7$. Thus, $2^{135} + 3^{98} + 5^{32} \equiv 1 + 2 + 4 \equiv 0 \pmod 7$, so it is indeed divisible by 7. □

(f) $n^2 + 2 = m^5 + 9$ has no integer solutions [Hint: try modulo 11]

This is true.

Proof. Consider squares and fifth powers modulo 11:

n	$n^2 \pmod{11}$	$n^5 \pmod{11}$
0	0	0
1	1	1
2	4	10
3	9	1
4	5	1
5	3	1
6	3	10
7	5	10
8	9	10
9	4	1
10	1	10

Therefore, modulo 11, n^2 must be congruent to one of 0,1,3,4,5 and 9, while m^3 must be congruent to one of 0,1 and 10. Therefore, $n^2 + 2$ will be congruent to one of 2,3,5,6,7 and 0, while $m^5 + 9$ must be congruent to one of 9,10, and 8. Therefore, the two quantities cannot be congruent modulo 11, so they cannot be equal. □

(g) For all natural numbers n, $\sum_{i=1}^{n} i^3 = \frac{n^2(n+1)^2}{4}$

This is true:

Proof. Induction on n. When $n = 0$, the sum is empty, so it is 0, while $\frac{n^2(n+1)^2}{4} = 0$ also, so the formula works.

Now suppose the formula works for n. We want to show that it works for $n+1$, i.e., we want to show that $\sum_{i=0}^{n+1} i^3 = \frac{(n+1)^2(n+2)^2}{4}$. However,

$$\sum_{i=0}^{n+1} i^3 = \sum_{i=0}^{n} i^3 + (n+1)^3 = \frac{n^2(n+1)^2}{4} + (n+1)^3$$
$$= (n+1)^2\left(\frac{n^2}{4} + n + 1\right) = (n+1)^2\frac{n^2+4n+4}{4} = \frac{(n+1)^2(n+2)^2}{4}$$

□

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

This is true.

Proof. Induction on n:

When $n = 0$, the formula obviously works.

Now suppose it works for n. We want to show that it also works for $n+1$, i.e. we want to show that $\sum_{i=1}^{n+1} \frac{1}{i(i+1)} = \frac{n+1}{n+2}$. Now

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

$\square$

(i) There are infinitely many primes congruent to 2 modulo 3. [Hint: suppose there are only finitely many; take the product of all of them. If this is congruent to 2 modulo 3, then multiply by 2. Add 1 to the resulting product. You may assume that any number that is congruent to 2 modulo 3 is divisible by a prime number congruent to 2 modulo 3.]

This is true.

Proof. Suppose there are only finitely many primes that are congruent to 2 modulo 3. Let them be $p_1, p_2, \ldots, p_k$. Now consider the product $N = p_1 p_2 \cdots p_k$. N is not divisible by 3, since none of the p_i is. Therefore, either $N \equiv 1 \pmod 3$ or $N \equiv 2 \pmod 3$. In the first case, $N + 1 \equiv 2 \pmod 3$, so it must be divisible by some prime that is congruent to 2 modulo 3, but it cannot be divisible by any prime that is congruent to 2 modulo 3, since all such primes divide N. In the second case, $2N + 1 \equiv 2 \pmod 3$, so it must be divisible by a prime that is congruent to 2 modulo 3. However, it cannot be divisible by a prime that is congruent to 2 modulo 3, since all such primes divide $2N$. Therefore, in either case we reach a contradiction, so our assumption that there were only finitely many such primes must be false, i.e., there must be infinitely many primes congruent to 2 modulo 3. $\square$

(j) For all natural numbers n, $\sum_{i=1}^{n}(i^3 - 3i) = \frac{n^4+2n^3-5n^2-6n+8}{4}$

This is false.

Proof. When $n = 0$, the sum is empty, so is 0, while $\frac{n^4+2n^3-5n^2-6n+8}{4} = \frac{8}{4} \neq 0$, so the formula does not hold when $n = 0$. $\square$

Note that the inductive step of a proof by induction works here, but the base case fails.

8 Find $0 \leqslant n < 660$ *satisfying all the following congruences:*

$$\begin{aligned} n &\equiv 3 \pmod 5 \quad (1)\\ n &\equiv 5 \pmod{11} \quad (2)\\ n &\equiv 4 \pmod{12} \quad (3) \end{aligned}$$

First we find $0 \leqslant n < 55$ satisfying the first two congruences. Observe that $11 \equiv 1 \pmod 5$, so $5 + 11n \equiv n \pmod 5$. Therefore, $5 + 11 \times 3 = 38$ satisfies the first two congruences.

Now we look for a solution to the two congruences:

$$\begin{aligned} n &\equiv 38 \pmod{55} \quad (4)\\ n &\equiv 4 \pmod{12} \quad (5) \end{aligned}$$

Note that $55 \equiv 7 \pmod 1)2$, so $55 \times 2 \equiv 2 \pmod{12}$. Thus, $38 + 55(2n) \equiv 2 + 2n \pmod{12}$, so $38 + 55 \times 2 \equiv 2 + 2 \equiv 4 \pmod{12}$, so $n = 148$ is the solution to the congruences.