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

Answer all questions.

1 Use Euclid's algorithm to find the greatest common divisor of 263 and 184. Write down all the steps involved. Use your calculations to find integers a and b such that $263a + 184b = (263, 184)$ times the second number is their greatest common divisor.

$$\begin{aligned} 263 &= 184 + 79 \\ 184 &= 2 \times 79 + 26 \\ 79 &= 3 \times 26 + 1 \\ 26 &= 26 \times 1 \end{aligned}$$

So $(263, 184) = 1$. Working backwards:

$$1 = 79 - 3 \times 26 = 79 - 3 \times (184 - 2 \times 79) = 7 \times 79 - 3 \times 184 = 7 \times (263 - 184) - 3 \times 184 = 7 \times 263 - 10 \times 184$$

So $a = 7$, $b = -10$ works.

2 Are the propositions $q \to (p \to r)$ and $p \to (q \to r)$ logically equivalent? Justify your answer.

The truth tables are as follows:

p	q	r	$p \to r$	$q \to (p \to r)$	$q \to r$	$p \to (q \to r)$
0	0	0	1	1	1	1
0	0	1	1	1	1	1
0	1	0	1	1	0	1
0	1	1	1	1	1	1
1	0	0	0	1	1	1
1	0	1	1	1	1	1
1	1	0	0	0	0	0
1	1	1	1	1	1	1

The fifth and last columns are the same, so the two propositions are logically equivalent.

3 *Which of the following are true when* $A = \{1, 2, 8\}$ *and* $B = \{0, 4, 5, 9, 17\}$*? Justify your answers.*

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

This is false. For example, $17 \in B$, but $17 + 1 = 18 \notin B$.

(b) $(\exists x \in A)(x + 3 \in A)$

This is false. For $x = 1$, $x + 3 = 4 \notin A$; for $x = 2$, $x + 3 = 5 \notin A$, and for $x = 8$, $x + 3 = 11 \notin A$.

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

This is false; Choose $x = 1$ ($x = 2$ and $x = 8$ can also work), and for the following values of y, the listed values of z make $x + y + z$ not prime:

y	z
0	8
4	1
5	2,8
9	2,8
17	2,8

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

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

$(\forall x \in A)(\neg(x \in B))$	Premise
$(\forall x)((x \in A) \rightarrow (\neg(x \in B)))$	Logical equivalence
$(y \in A) \rightarrow (\neg(y \in B))$	Universal instantiation
$(y \in A \vee y \in C) \wedge (y \in B \vee y \in C)$	Premise
$(y \in B) \vee (y \in C)$	Specialisation
$(\neg(y \in B)) \rightarrow (y \in C)$	Logical equivalence
$(y \in A) \rightarrow (y \in C)$	Transitivity from 3 & 6
$(y \in C) \rightarrow (y \in C)$	Tautology
$(y \in A) \vee (y \in C)$	Specialisation from 4
$y \in C$	Division into cases

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

(a) There is a natural number n such that $n^2 + 5n - 6$ is prime.

This is false.

Proof. $n^2 + 5n - 6 = (n + 6)(n - 1)$, so if neither $n + 6$ nor $n - 1$ is ± 1, then $n^2 + 5n - 6$ is composite. If $n + 6 = 1$, then $n - 1 = -6$, which is not prime; if $n + 6 = -1$, then $n - 1 = -8$, which is not prime; if $n - 1 = 1$, then $n + 6 = 8$, which is not prime; finally if $n - 1 = -1$, then $n + 6 = 6$, which is not prime. □

(b) $2^{19} + 3^8 + 7^{84}$ is divisible by 5.

This is true. $2^2 \equiv 4 \pmod 5$, $2^4 \equiv 4^2 \equiv 1 \pmod{}()5$, so $2^{16} \equiv 1^4 \equiv 1 \pmod 5$, so $2^{19} \equiv 2^3 \equiv 3 \pmod 5$. $3^2 \equiv 4 \pmod 5$, so $3^4 \equiv 1 \pmod 5$, so $3^8 \equiv 1 \pmod 5$. Finally, $7 \equiv 2 \pmod 5$, so $7^{84} \equiv 2^8 4 \equiv 1^2 1 \equiv 1 \pmod 5$. Therefore, $2^{19} + 3^8 + 7^{84} \equiv 3 + 1 + 1 \equiv 0 \pmod 5$. Thus $2^{19} + 3^8 + 7^{84}$ is divisible by 5.

6 Find $0 \leqslant n < 770$ satisfying all the following congruences:

$$\begin{aligned} n &\equiv 4 \pmod{11} && (1)\\ n &\equiv 2 \pmod{14} && (2)\\ n &\equiv 3 \pmod 5 && (3) \end{aligned}$$

For the first two congruences:

$$\begin{aligned} n &\equiv 4 \pmod{11}\\ n &\equiv 2 \pmod{14} \end{aligned}$$

We observe that $4 \times 14 - 5 \times 11 = 1$, so $4 \times 14 \equiv 1 \pmod{11}$. $n = 2 + 14k$ for some integer k, from the second congruence. Therefore, $2 + 14k \equiv 4 \pmod{11}$, so $14k \equiv 2 \pmod{11}$, which gives $k \equiv 4 \times 2 = 8 \pmod{11}$, so $n \equiv 2 + 14 \times 8 \equiv 114 \pmod{}()11 \times 14 = 154)$ is the solution to the first two congruences.

Now we need to solve:

$$\begin{aligned} n &\equiv 114 \pmod{154} && (4)\\ n &\equiv 3 \pmod 5 && (5) \end{aligned}$$

This gives $n = 114 + 154k \equiv 4 + 4k \pmod 5$, so $4 + 4k \equiv 3 \pmod 5$, which gives $k \equiv 1 \pmod 5$, so $n = 114 + 154 = 268$ is a solution.

7 Solve the following recurrence relations:

(a) $a_n = a_{n-1} + 2a_{n-2}$, $a_0 = 1$, $a_1 = 3$.

This is a second-order homogeneous constant-coefficient linear recurrence, so we look for solutions of the form $a_n = t^n$. This gives the equation $t^2 = t + 2$, so $t = 2$ and $t = -1$ are solutions. The general solution is therefore of the form $a_n = A2^n + B(-1)^n$. To find A and B, we substitute the values of a_0 and a_1, to get:

$$A + B = 1 \quad (6)$$
$$2A - B = 3 \quad (7)$$

This gives $A = \frac{4}{3}$, $B = -\frac{1}{3}$, so the general solution is $a_n = \frac{2^{n+2} + (-1)^{n+1}}{3}$.

(b) $a_n = 6a_{n-1} - 9a_{n-2}$, $a_0 = 0$, $a_1 = 4$.

This is a second-order homogeneous constant-coefficient linear recurrence, so we look for solutions of the form $a_n = t^n$ for some t. We get the equation $t^2 = 6t - 9$, which gives $t = 3$ as a double solution. Therefore, $a_n = 3^n$ and $a_n = n3^n$ both satisfy the recurrence, so the general solution is $a_n = (An + B)3^n$. We substitute the values for a_0 and a_1 to get $B = 0$, and $3A = 4$, so the solution is $a_n = 4n3^{n-1}$.

(c) $a_n = 2a_{n-1} + 3$, $a_0 = 3$.

We start by looking at the first few values for a_n:

n	a_n
0	3
1	9
2	21
3	45

This suggests $a_n = 3(2^{n+1} - 1)$ is the general formula. We check this by induction. For $n = 0$, we have already checked that the formula works. Suppose it works for n, i.e. $a_n = 3(2^{n+1} - 1)$, we want to show that $a_{n+1} = (2^{n+2} - 1)$. By the recurrence relation, $a_{n+1} = 2a_n + 3 = 6(2^{n+1} - 1) + 3 = 3(2^{n+2} - 2 + 1) = 3(2^{n+2} - 1)$ as required. Therefore, by induction, the formula works for all n.

8 Show by induction on n that if A is a set of n elements, then its power set $\mathcal{P}(A)$ has 2^n elements. [Hint: let $a \in A$, and consider $\mathcal{P}(A)$ as the union

of the set of subsets of A that contain a, and the set of subsets of A that don't contain a.]

Proof. When $n = 0$, A is the empty set $\emptyset$, so its power set has just one element, $\emptyset$, so the result holds. Now suppose that the result holds for n, and suppose that A is a set with $n+1$ elements. Let $a \in A$. Then $A \setminus \{a\}$ is a set with n elements, so by our induction hypothesis, $\mathcal{P}(A \setminus \{a\})$ has 2^n elements. If A' is a subset of A, then either $x \in A'$, in which case $A' \setminus \{a\} \subseteq A \setminus \{a\}$, or $x \notin A'$, in which case $A' \subseteq A \setminus \{a\}$. On the other hand, if $X \subseteq A \setminus \{a\}$, then X and $X \setminus \{a\}$ are both subsets of A, so there are 2^n subsets of A that contain a, and 2^n that don't contain a. Therefore, there are a total of 2^{n+1} subsets of a (there are no subsets of A that both contain a and don't contain a). Therefore, the result holds for all $n \in \mathbb{N}$ by induction. □

9 Let $A = \{0, 1, 3, 7\}$, $B = \{1, 2, 7, 8\}$. What are:
(i) $A \cup B$?

$A \cup B = \{0, 1, 2, 3, 7, 8\}$

(ii) $A \cap B$?

$A \cap B = \{1, 7\}$

(iii) $A \times B$?

$A \times B = \{(0,1), (0,2), (0,7), (0,8), (1,1), (1,2), (1,7), (1,8), (3,1), (3,2), (3,7), (3,8), (7,1), (7,2), (7,7), (7,8)\}$

(iv) $B \setminus A$?

$B \setminus A = \{2, 8\}$

10 Let A, B, and C be sets such that $|A| = 7$, $|B| = 9$, $|C| = 17$, $|A \cap B| = 4$, $|A \cap C| = 3$, $|B \cap C| = 7$, and $|A \cup B \cup C| = 21$. What are the possible values for $|A \cap B \cap C|$?

By the inclusion-exclusion principle, $|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|$, so $21 = 7+9+17-4-3-7+|A \cap B \cap C|$, so $|A \cap B \cap C| = 2$.

11 For each of the following relations, determine which of the properties: reflexivity, symmetry, transitivity, and antisymmetry hold:

(a) The relation R on the set of all sets given by $A\ R\ B$ if and only if $\emptyset \in A \wedge \emptyset \in B$.

This is not reflexive, since if $\emptyset \notin A$, then A is not related to A. It is symmetric, since if $\emptyset \in A \wedge \emptyset \in B$, then $\emptyset \in B \wedge \emptyset \in A$. It is not antisymmetric, since for example, if $A = \{\emptyset\}$, and $B = \{1, \emptyset\}$, then $A\ R\ B$ and $B\ R\ A$, but $A \neq B$. Finally, it is transitive, since if $A\ R\ B$, and $B\ R\ C$, then by specialisation, we get $\emptyset \in A$, and $\emptyset \in C$, so by conjunction we get $\emptyset \in A \wedge \emptyset \in C$, so $A\ R\ C$.

(b) The relation R on the set of natural numbers given by $n\ R\ m$ if and only if $n|m$.

This is reflexive, since for any $n \in \mathbb{N}$, $n = 1 \times n$, so $n|n$. It is not symmetric, for example, $2|4$, but 4 does not divide 2. It is antisymmetric, since if $m|n$ and $n|m$, then there are natural numbers k and l such that $n = km$ and $m = ln$, so $m = klm$, so either $m = 0$, in which case $n = m$, or $kl = 1$, which means that $k = l = 1$, so $n = m$. It is transitive, by transitivity of divisibility.

(c) The relation R on the set of all natural numbers given by $m\ R\ n$ if and only if m is odd and n is even.

This is not reflexive, since there are natural numbers which are not both odd and even – any natural number provides a counterexample. It is not symmetric, since for example, $1\ R\ 2$, but 2 is not related to 1. It is antisymmetric, since if $m\ R\ n$, then n is even, so it is not odd, so n is not related to any natural number, so in particular, it is not related to m. It is also transitive, since the conditions $m\ R\ n$ and $n\ R\ l$ can never both hold.

(d) The relation R on the set of positive rational numbers given by $q\ R\ r$ if $q = \frac{a}{b}$, $r = \frac{c}{d}$ with $(a, b) = (c, d) = 1$, $a, b, c, d \in \mathbb{Z}^+$ and $ad < b$.

This is not reflexive, since, for example, if $q = \frac{1}{2}$, then q is not related to itself, since $1 \times 2 \geqslant 2$. It is not symmetric. For example, if $q = \frac{1}{7}$, and $r = \frac{3}{4}$, then $q\ R\ r$, but r is not related to q. It is antisymmetric, since if $\frac{a}{b}\ R\ \frac{c}{d}\ R\ \frac{a}{b}$, where $(a, b) = (c, d) = 1$, then $ad < b \leqslant bc < d$, which can't happen, since $a \geqslant 1$.

12 (a) Which of the following functions are injective? (b) Which are surjective?

(i) $f : \mathbb{R}^+ \to \mathbb{R}^+$, $f(x) = x^2$.

f is injective, since if $x^2 = y^2$, then $x^2 - y^2 = 0$, so $(x + y)(x - y) = 0$, giving $x = y$ or $x = -y$. $x = -y$ is impossible, since x and y are both positive, so $x = y$. f is surjective, since for any $y \in \mathbb{R}^+$, $f(\sqrt{y}) = y$.

(ii) $f : \mathbb{R} \to \mathbb{R}$, $f(x) = x^2$.

f is not injective, since for example, $f(-1) = 1 = f(1)$. f is not surjective since there is no $x \in \mathbb{R}$ such that $x^2 = -1$.

(iii) $f : \mathbb{N} \to \{0, 1\}$, $f(n) = \begin{cases} 0 & \text{if } n \text{ is prime} \\ 1 & \text{otherwise} \end{cases}$.

f is not injective, since $f(2) = f(3) = 0$. f is surjective, since $f(1) = 1$ and $f(2) = 0$.

(iv) $f : \mathbb{Q} \to \mathbb{R}$, $f(x) = 2x$.

f is injective, since if $f(x) = f(y)$, then $2x = 2y$, so $x = y$. f is not surjective, since for example, there is no rational number q with $2q = \sqrt{2}$ (since $\frac{\sqrt{2}}{2}$ is irrational).

13 Show by strong induction that every positive integer congruent to 2 modulo 3 is divisible by a (positive) prime number congruent to 2 modulo 3.

Proof. The result holds for 2, since 2 is prime. Now suppose that every $n \equiv 2 \pmod 3$ with $n < N$ for some $N \equiv 2 \pmod 3$ is divisible by a prime $p \equiv 2 \pmod 3$. We want to show that N is divisible by a prime $p \equiv 2 \pmod 3$. If N is prime, then it is divisible by itself. If not, then $N = ab$ for $1 < a, b < N$. If a and b are both congruent to either 0 or 1 modulo 3, then N would also be congruent to 0 or 1. Therefore, at least one of a and b must be congruent to 2 modulo 3. W.L.O.G. let $a \equiv 2 \pmod 3$. Since $a < N$, by our induction hypothesis, a is divisible by a prime $p \equiv 2 \pmod 3$, so $p|N$, and the result holds for N. Therefore, by strong induction, it holds for all $n \in \mathbb{N}$. □

14 Show that it is not possible to write a computer program which takes as input a computer program P, and some value X, and determines whether the programs P eventually finishes when given input X.

Proof. Suppose we have a computer program H which inputs a computer program P and a value X, and determines whether P finishes with input X. We can use it to write a program Q that inputs a program P, determines whether P finishes when it's input is P (i.e. runs $H(P, P)$ and looks at the output) and if P does terminate with input P, Q starts an infinite loop (so it never terminates), while if P does not terminate with input P, Q terminates. Now consider what happens when Q is run with input Q. In order to terminate, it must determine that Q does not terminate when given Q as input, in which case it can't terminate. On the other hand, if it doesn't terminate, then $H(Q, Q)$ will determine that it doesn't terminate, so Q terminate once H does. This is a contradiction, so our assumption that the program H exists must be false, and there can be no such program. □

15 Consider the following algorithm, called a bubble sort for sorting a list $a[1], a[2], \ldots, a[n]$ of length n.

Algorithm 1 Bubble Sort

Input: List $a[1], a[2], \ldots, a[n]$
Output: Sorted list $a[1], a[2], \ldots, a[n]$

```
numSwaps=1
while numSwaps>0 do
  numSwaps=0
  for i=1 to n-1 do
    Compare a[i] to a[i + 1]
    if a[i] > a[i + 1] then
      swap a[i] and a[i+1]
      numSwaps=numSwaps+1
    end if
  end for
end while
```

How many comparisons does it make to sort a list of length n: (Give your answers in the form $\Theta(f(n))$ for some function f), justify your answers.

(a) In the best case?

Each iteration of the outer loop performs $n-1$ comparisons, so the question is how many times is the outer loop iterated? It runs until no swaps were required. If the list is initially sorted, then no swaps will be required on the first iteration of the outer loop, so the loop will only be iterated once. Therefore, only $n - 1 = \Theta(n)$ comparisons will be performed.

(b) In the worst case? [Hint: Every time the outer loop runs, we know that for every $i < n$, there is at least one more $j > i$ with $a[j] > a[i]$.]

If the outer loop has been iterated k times for some natural number k, then for any $i \leqslant n-k$, there must be at least k elements $a[j]$ of the current list with $i < j$ and $a[i] < a[j]$. We can prove this by induction on k: if $k = 0$, the result is trivially true. Suppose the result is true for one value of k. We want to show that when we run the loop one more time, there will be at least $k+1$ elements $a[j]$ such that $j > i$ and $a[j] > a[i]$. The element that ends up in the ith position after the $(k+1)$th iteration of the loop must be smaller than the element that was in the $(i+1)$th position after k iterations. This element is, by the inductive hypothesis, smaller than k of the $a[j]$ with $j > i+1$, so these k elements are also bigger than $a[i]$, and after the $(k+1)$th iteration, they are still after $a[i]$ in the list, so the result holds for $k+1$, so by induction, it holds for all k.

Therefore, after $n-1$ iterations, the list will be sorted, so no swaps will be made on the nth iteration, so the program will finish after at most n iterations of the outer loop. Therefore, it performs a total of $n(n-1) = \Theta(n^2)$ comparisons.

16 Define the function $F : \mathbb{N} \to \mathbb{N}$ recursively by:

$$F(n) = \begin{cases} 4F\left(\frac{n}{2}\right) & \text{if } n \text{ is even.} \\ F(n-1) + 2n - 1 & \text{if } n \text{ is odd} \end{cases}$$

and $F(0) = 0$.

Find a formula for $F(n)$, and prove it.

We start by looking at the first few values of $F(n)$:

n	$F(n)$
0	0
1	1
2	4
3	9

This leads us to conjecture that $F(n) = n^2$. We prove this by strong induction:

Proof. We have already checked that the formula works for $n = 0$. Now suppose it holds for all natural numbers $n < k$ $(k > 0)$. We need to show that it also holds for $n = k$. If k is even then $F(k) = 4F\left(\frac{k}{2}\right) = 4\left(\frac{k}{2}\right)^2 = k^2$, so the result holds. If k is odd then $F(k) = F(k-1) + 2k - 1 = (k-1)^2 + 2k - 1 = k^2$, so the result holds for $n = k$. Thus by induction, it holds for all n. □

17 Given a set X of 10 natural numbers $\{n_1, \ldots, n_{10}\}$, for a non-empty subset X' of X, define $S_{X'} = \sum_{i \in X'} n_i$. show that there are two non-empty subsets X_0 and X_1 of X such that $S_{X_0} \equiv S_{X_1} \pmod{1000}$.

Proof. Since X has 10 elements, it has $2^{10} = 1024$ subsets. 1023 of these are non-empty. On the other hand, $S_{X'}$ can only take 1000 values modulo 1000, so some two non-empty subsets X_0 and X_1 must have $S_{X_0} \equiv S_{X_1} \pmod{1000}$ by the pigeon-hole principle. □