University of Ottawa
CSI 2101 – Midterm Test
Instructor: Lucia Moura

March 1, 2012
1:00 pm
Duration: 1:15 hs

Closed book, no calculators

Last name: _____

First name: _____

Student number: _____

There are 4 questions and 100 marks total.

This exam paper should have 9 pages,
including this cover page.

1 – Predicate logic	/ 30
2 – Inference rules	/ 20
3 – Proof Methods	/ 20
4 – Number Theory	/ 30
Total	/ 100

1 Predicate logic — 30 points

Part A — 12 points

Circle true or false

$\forall n \exists m(n - m = 0)$, where the domain is the set of natural numbers.	**[true]**	[false]
$\exists n \forall m(n - m = 0)$, where the domain is the set of natural numbers.	[true]	**[false]**
The following are logically equivalent: $\neg(p \wedge \neg q)$ and $(p \rightarrow q)$	**[true]**	[false]
The following are logically equivalent: $\exists x \neg Q(x)$ and $\neg \forall x \neg Q(x)$	[true]	**[false]**
The following are logically equivalent: $\neg \forall x \exists y P(x, y)$ and $\exists x \forall y \neg P(x, y)$	**[true]**	[false]
Consider the universe of discourse to be the set $\{1, 2, 3\}$, and $Q(x, y) =$"$y \geq x$". Then $\exists y \forall x Q(x, y)$ is true.	**[true]**	[false]

Part B — 18 points

Assume the universe of discourse to be all people, and the following statements:

$D(x)$: "x is a duck."
$O(x)$: "x is an officer."
$W(x)$: "x is willing to waltz."

Translate each of the following phrases using quantifiers, logical connectives and $D(x)$, $O(x)$ and $W(x)$.

	phrase in English	logical statement
1.	No ducks are willing to waltz.	$\neg \exists (D(x) \wedge W(x)) \equiv \forall x (D(x) \rightarrow \neg W(x))$
2.	No officers ever decline to waltz.	$\neg \exists (O(x) \wedge \neg W(x)) \equiv \forall x (O(x) \rightarrow W(x))$
3.	Ducks are not officers.	$\forall x (D(x) \rightarrow \neg O(x))$

For each of the English phrases above, write its negation in English.
Then, translate each of the negated English phrases into predicate logic; make sure the logical statement you write has the $\neg$ connectives applied to individual propositional functions only ($D(x)$, $O(x)$ or $W(x)$), that is, no $\neg$ connective is outside quantifiers or outside expressions involving other connectives.

	negated English prases	logical statement
1.	Some ducks are willing to waltz.	$\exists x (D(x) \wedge W(x))$
2.	Some officers decline to waltz.	$\exists x (O(x) \wedge \neg W(x))$
3.	Some ducks are officers.	$\exists x (D(x) \wedge O(x))$

... continued

2 Inference rules — 20 points

Part A — 10 points Use a formal proof and rules of inference to show that if the premises $\forall x(P(x) \rightarrow (Q(x) \wedge S(x)))$ and $\forall x(P(x) \wedge R(x))$ are true, then the conclusion $\forall x(R(x) \wedge S(x))$ is true.

Formal Proof:

Step	Reason
1. $\forall x(P(x) \wedge R(x)$	hypothesis
2. $P(a) \wedge R(a)$ for arbitrary a	universal instantiation of 2
3. $P(a)$	simplification of 2
4. $R(a)$	simplification of 2
5. $\forall x(P(x) \rightarrow (Q(x) \wedge S(x))$	hypothesis
6. $P(a) \rightarrow (Q(a) \wedge S(a))$	universal instantionation of 5
7.$Q(a) \wedge S(a)$	modus ponens of 3 and 6
8. $S(a)$	simplification of 7
9. $R(a) \wedge S(a)$	conjunction of 4 and 8
10. $\forall x(R(x) \wedge S(x))$	universal generalization of 9

... continued

Part B — 10 points Determine if the argument is correct or not using the steps below.

The premises:
"Every person attends a school that is not expensive or lives in a basement."
"Every person is smart or attends an expensive school."

yield the conclusion that

"Each person is smart or lives in a basement."

- (4 points) Define the required predicates needed in the next part to express the premises and conclusions in predicate logic.

  $E(x)$: "x attends an expensive school."

  $B(x)$: "x lives in a basement."

  $S(x)$: "x is smart."

- (4 points) Write the rule that expresses that the premises lead to the conclusion. That is, express the premises and conclusions in predicate logic in the format of a rule of inference.

$$\frac{\begin{array}{c}\forall x(\neg E(x) \vee B(x)) \\ \forall x(S(x) \vee E(x))\end{array}}{\therefore \forall x(S(x) \vee B(x))}$$

- (2 points) Is the argument above correct?

  Yes. It can be derived from the application of universal instantiation, rule of resolution, followed by universal generalization.

... continued

3 Proof Methods — 20 points

Part A — 10 points Use a proof by contraposition to prove the following theorem.

Let a, b, c be positive integers. If $n = abc$ then $a \leq \sqrt[3]{n}$ or $b \leq \sqrt[3]{n}$ or $c \leq \sqrt[3]{n}$.

Proof by contraposition:

Assume $a > \sqrt[3]{n}$, $b > \sqrt[3]{n}$ and $c > \sqrt[3]{n}$.
(this is the negation of $a \leq \sqrt[3]{n}$ *or* $b \leq \sqrt[3]{n}$ *or* $c \leq \sqrt[3]{n}$*).*

So $abc > \sqrt[3]{n} \cdot \sqrt[3]{n} \cdot \sqrt[3]{n} = n$.

Thus $abc \neq n$. *(this is the negation of* $n = abc$*).*

... continued

Part B — 10 points

Prove the following:

For any integer number n, if $3n^3 + 5$ is odd then n is even.

using

B1 (5 points) a proof by contraposition.

Assume n is odd, i.e. there exists an integer k such that $n = 2k + 1$.
So,

$$\begin{aligned} 3n^3 + 5 &= 3(2k+1)^3 + 5 \\ &= 3\left[(2k)^3 + 3(2k)^2 + 3(2k) + 1^3\right] + 5 \\ &= 2(3(2^2k^3) + 3^2 2k^2 + 3^2 k + 4). \end{aligned}$$

So, there exists $k' = 3(2^2k^3) + 3^2 2k^2 + 3^2 k + 4$, such that $3n^3 + 5 = 2k'$.

Therefore, $3n^3 + 5$ is even.

B2 (5 points) a proof by contradiction.

Assume $3n^3 + 5$ is odd and n is odd.
(note that the negation of $\forall n(P(n) \rightarrow Q(n)$ *is equivalent to* $\exists n(P(n) \wedge \neg Q(n)))$

So $n = 2k + 1$ for some integer k. Similarly to part a, we derive:

$$\begin{aligned} 3n^3 + 5 &= 3(2k+1)^3 + 5 \\ &= 3\left[(2k)^3 + 3(2k)^2 + 3(2k) + 1^3\right] + 5 \\ &= 2(3(2^2k^3) + 3^2 2k^2 + 3^2 k + 4). \end{aligned}$$

So, there exists $k' = 3(2^2k^3) + 3^2 2k^2 + 3^2 k + 4$, such that $3n^3 + 5 = 2k'$.

The hypothesis that $3n^3 + 5$ is odd also gives us $3n^3 + 5 = 2k'' + 1$, for some integer k''.

So, $3n^3 + 5 = 2k' = 2k'' + 1$, which implies $1 = 2(k' - k'')$, where k', k'' are integers.

Thus, 2 divides 1 (or equivalently 1 is even), which is a contradiction.

... continued

4 Number Theory — 30 points

Part A — 10 points Use the Chinese Remainder Theorem to find all solutions to he system of congruences:

$$\begin{aligned} x &\equiv 2 \pmod 3 \\ x &\equiv 1 \pmod 4 \\ x &\equiv 3 \pmod 5 \end{aligned}$$

$M_1 = m_2 m_3 = 20$,
y_1 is the inverse of 20 mod 3, which is the same as the inverse of 2 mod 3, so $y_1 = 2$.
$M_2 = m_1 m_3 = 15$,
y_2 is the inverse of 15 mod 4, which is the same as the inverse of 3 mod 4, so $y_2 = 3$.
$M_3 = m_1 m_2 = 12$,
y_3 is the inverse of 12 mod 5, which is the same as the inverse of 2 mod 5, so $y_3 = 3$.

$$\begin{aligned} x &\equiv a_1 M_1 y_1 + a_2 M_2 y_2 + a_3 M_3 y_3 \pmod{60} \\ &\equiv 2 \cdot 20 \cdot 2 + 1 \cdot 15 \cdot 3 + 3 \cdot 12 \cdot 3 \pmod{60} \\ &\equiv 233 \equiv 53 \pmod{60} \end{aligned}$$

So the solutions to the system of congruences are:
$x = 53 + 60k$, for all integers k.

... continued

Part B — 10 points Prove the following result.

> Let $m_1, m_2, \ldots, m_n$ be pairwise relatively prime integers greater than equal to 2, and let $m = m_1 m_2 \cdots m_n$. Show that if $a \equiv b \pmod{m_i}$ for all $1 \leq i \leq n$ then $a \equiv b \pmod{m}$.

Note: do not use the Chinese Remainder Theorem because its proof makes use of this result.

Proof 1:

We will use the following claim: If $x|c$ and $y|c$ and $gcd(x, y) = 1$ then $xy|c$.
Proof the the claim:
$y|c$ implies there exists an integer k such that $c = ky$.
So, $x|ky$. By Lemma A seen in class, since $gcd(x, y) = 1$ we conclude $x|k$, or in other words $k = dx$ for some integer d. So, $c = ky = dxy$. Therefore $xy|c$. So the claim is proven.

Now, since $a \equiv b \pmod{m_i}$, for all $1 \leq i \leq n$, we know that $m_i|(a - b)$, for all $1 \leq i \leq n$.

Applying the claim above iteratively for $c = (a - b)$, we conclude successively that $m_1 m_2|(a - b)$, $(m_1 m_2)m_3|(a - b)$,...,$(m_1 m_2 \cdots m_{n-1})m_n|(a - b)$.
Thus $m|(a - b)$, which implies $a \equiv b \pmod{m}$.

Proof 2 (alternative):
Consider the unique prime factorization of each of $m_1, m_2, \ldots, m_n$, say

$$m_i = p_{i,1}^{e_{i,1}} p_{i,2}^{e_{i,2}} \cdots p_{i,s_i}^{e_{i,s_i}}$$

Since $m_i|(a - b)$ then each $p_{i,1}^{e_{i,1}}, p_{i,2}^{e_{i,2}}, \ldots, p_{i,s_i}^{e_{i,s_i}}$ appears in the prime factorization of $(a - b)$, for all $1 \leq i \leq n$.

Since $gcd(m_j, m_k) = 1$, for all $1 \leq j, k \leq n$, $j \neq k$, we know that all the $p_{i,l}$ are distinct of each other.

So $p_{1,1}^{e_{1,1}}, p_{1,2}^{e_{1,2}}, \ldots, p_{1,s_1}^{e_{1,s_1}}, p_{2,1}^{e_{2,1}}, p_{2,2}^{e_{2,2}}, \ldots, p_{2,s_2}^{e_{2,s_2}}, \ldots, p_{n,1}^{e_{n,1}}, p_{n,2}^{e_{n,2}}, \ldots, p_{n,s_n}^{e_{n,s_n}}$ are all distinct prime powers that appear in the prime factorization of $(a - b)$.

Thus,

$$(a - b) = (p_{1,1}^{e_{1,1}} p_{1,2}^{e_{1,2}} \ldots p_{1,s_1}^{e_{1,s_1}} p_{2,1}^{e_{2,1}} p_{2,2}^{e_{2,2}} \ldots, p_{2,s_2}^{e_{2,s_2}} \ldots, p_{n,1}^{e_{n,1}} p_{n,2}^{e_{n,2}} \ldots, p_{n,s_n}^{e_{n,s_n}})x$$

for some integer x, or equivalently

$$(a - b) = (m_1 m_2 \cdots m_n)x = mx.$$

Therefore, $m|(a - b)$, which implies $a \equiv b (\mathrm{mod} m)$.

... continued

Part C — 10 points RSA

Consider the RSA cryptosystem with $p = 17$, $q = 19$ and $e = 7$.

Bob calculates $n = p \times q = 17 \times 19 = 323$, and publishes his public key $(n = 323, e = 7)$.

(a) (3 marks) How does Bob calculate his private key? Please, simply state what needs to be calculated.

Answer: Bob's private key consists of a pair $(n = 323, d)$ where d is the inverse of e (mod $(p-1)(q-1)$), i.e. the inverse of 7 (mod 288).

(b) (3 marks) Perform the necessary calculations and compute the private key.

Answer:

Using the extended Euclidean algorithm, we get $288 = 41 \times 7 + 1$ and then $gcd(288, 7) = 1 = 288 - 41 \times 7$.

So $d \equiv -41 \equiv 247 \pmod{288}$.

Bob's private key is $(n = 323, d = 247)$

(c) (4 marks) State encoding and decoding equations. Explain how to encode the plaintext given as the number 99 and how to decode the ciphertext given as the number 101.

You do not need to do any calculations; just state the equations for these particular plaintext and ciphertext.

Answer:

$$E(99) = 99^7 \pmod{323}$$
$$D(101) = 101^{247} \pmod{323}$$

... End Of Midterm Test