Midterm - 02/15/'06

Part I

Exercise 1

a) Truth table for $(p \to \neg p) \to \neg p$:

p	$\neg p$	$q = p \to \neg p$	$q \to \neg p$
F	T	T	T
T	F	F	T

$>$ From Column 4, $(p \to \neg p) \to \neg p$ is a tautology.

b) Truth table for $(p \wedge \neg p) \leftrightarrow (q \wedge \neg q)$:

p	q	$a = p \wedge \neg p$	$b = q \wedge \neg q$	$a \to b$	$b \to a$	$a \leftrightarrow b$
F	F	F	F	T	T	T
F	T	F	F	T	T	T
T	F	F	F	T	T	T
T	T	F	F	T	T	T

$>$ From Column 7, $(p \wedge \neg p) \leftrightarrow (q \wedge \neg q)$ is a tautology.

c) Truth table for $(p \vee \neg p) \leftrightarrow (q \vee \neg q)$:

p	q	$a = p \vee \neg p$	$b = q \vee \neg q$	$a \to b$	$b \to a$	$a \leftrightarrow b$
F	F	T	T	T	T	T
F	T	T	T	T	T	T
T	F	T	T	T	T	T
T	T	T	T	T	T	T

$>$ From Column 7, $(p \vee \neg p) \leftrightarrow (q \vee \neg q)$ is a tautology.

Exercise 2

a) Let us consider the composite statement:
$u = (p \wedge q) \vee (p \wedge \neg q) \vee (\neg p \vee q) \vee (\neg p \vee \neg q)$.
Let us define $r = p \wedge q$ and $s = p \wedge \neg q$. According to deMorgan's law, $\neg r = \neg p \vee \neg q$ and $\neg s = \neg p \vee q$. We can therefore rewrite the original statement u as:
$u = r \vee s \vee \neg s \vee \neg r$.
Based on the negation law $s \vee \neg s \Leftrightarrow T$, and $r \vee \neg r \Leftrightarrow T$. Therefore,
$u \Leftrightarrow T$, i.e. u is a tautology.

b) Using in this order: the associativity of $\wedge$ and $\vee$, the negation law, and the identity law, we get

$$\begin{aligned}(p \wedge q) \vee (p \wedge \neg q) \vee (\neg p \wedge q) \vee (\neg p \wedge \neg q) &\Leftrightarrow (p \wedge (q \vee \neg q)) \vee (\neg p \wedge (q \vee \neg q)) \\ &\Leftrightarrow (p \wedge T) \vee (\neg p \wedge T) \\ &\Leftrightarrow p \vee \neg p \\ &\Leftrightarrow T\end{aligned}$$

Hence the original statement is a tautology.

Part II

Exercise 1

To prove that n is even if and only if $5n^2+2$ is even, we have to prove the two following implications:

- If n is even, $5n^2+2$ is even : Let $n = 2k$. Then, $5n^2+2 = 5*4k^2+2 = 2(10k^2+1)$. Since $5n^2+2$ is a multiple of 2, it is even. Hence by direct proof, we proved that if n is even, $5n^2+2$ is even.

- If $5n^2+2$ is even, n is even. We will use an indirect proof. Let us assume that n is odd, i.e. there exists k such that $n = 2k+1$. Then $5n^2+2 = 5*(2k+1)^2+2 = 5(4k^2+4k+1)+2 = 20k^2+20k+7 = 2(10k^2+10k+3)+1 = 2k'+1$ by defining $k' = (10k^2+10k+3)$. Thus, we get $5n^2+2$ to be odd as it is not a multiple of 2. We have proved that if n is odd, then $5n^2+2$ is odd, which validates its contrapositive, i.e. if $5n^2+2$ is even, then n is even.

Since we have proved that if n is even, $5n^2+2$ is even and its converse, we can conclude that n is even if and only if $5n^2+2$ is even.

Exercise 2

Since x, y, and z are natural numbers greater than 1, the number (xyz+1) is not divisible by either x, y or z, as xyz is a multiple of all of the three numbers, and (xyz+1)≡ 1(mod x), (xyz+1)≡ 1(mod y) and (xyz+1)≡ 1(mod z). Thus, we have proved by constructive proof that there exists at least one number greater than x, y, and z, which is not divisible by either of the three.

Exercise 3

Let p be the proposition "n^2 is not divisible by 4", and q be the proposition "n is odd". To prove the implication $p \to q$, we use an indirect proof, i.e. we will prove the contrapositive $\neg q \to \neg p$. $\neg q$ is the proposition "n is even", and $\neg p$ is the proposition " n^2 is a multiple of 4"'.
Let us assume n is even. Then there exists k such that $n = 2k$. Consequently, $n^2 = 4k^2$, i.e. n^2 is a multiple of 4. This concludes the proof.

Exercise 4

Given $a = 2^{1001} - 5^{701} + 7^{256}$, $b = 2^{1001} - 5^{701} + 7^{256} - 1$, and $c = 2^{1001} - 5^{701} + 7^{256} + 1$, we find that $a = b+1$, and $c = a+1 = b+2$. b, a and c are therefore 3 consecutive integers. There are two possibilities for b:

- b is even: Then, b is a multiple of 2 (note that $c = b+2$ is also a multiple of 2).

- b is odd: Then, $a = b+1$ is even, i.e. a is a multiple of 2.

Similarly, there are three possibilities for b when it is divided by 3:

- b is divisible by 3: Then, b is a multiple of 3.

- The remainder of the division of b by 3 is 1: There exists k $\in \mathbb{Z}$ such that $b = 3k+1$. Then $c = b+2 = 3k+3 = 3(k+1)$: c is a multiple of 3.

- The remainder of the division of b by 3 is 2: There exists k $\in \mathbb{Z}$ such that $b = 3k+2$. Then $a = b+1 = 3k+3 = 3(k+1)$: a is a multiple of 3.

Thus, for any situation, at least one of the three numbers a, b, c is a multiple of 2 and at least one of them is a multiple of 3. We have used a non-constructive proof as we do not know which one is a multiple of 2, and which one is a multiple of 3.

Exercise 5

a) We know that $10 \equiv 0 (\text{mod } 2)$, as, 10 is a multiple of 2. Consequently, $10^k \equiv 0 (\text{mod } 2)$, for all $k \geq 1$. Then

$$\begin{aligned} n &\equiv (a_p 10^p + a_{p-1} 10^{p-1} + \ldots + a_0) (\text{mod } 2) \\ &\equiv a_0 (\text{mod } 2) \end{aligned} \tag{1}$$

Thus, $a_0 \equiv 0 (\text{mod } 2) \Rightarrow n \equiv 0 (\text{mod } 2)$. Thus, divisibility of n by 2 is decided by the divisibility of a_0 by 2. Hence, n is divisible by 2, only if a_0 is equal to 0, 2, 4, 6 or 8.

b) We know that $100 \equiv 0 (\text{mod } 4)$, as, 100 is a multiple of 4. Consequently, $10^k \equiv 0 (\text{mod } 2)$, for all $k \geq 2$. Then

$$\begin{aligned} n &\equiv (a_p 10^p + a_{p-1} 10^{p-1} + \ldots + a_0) (\text{mod } 4) \\ &\equiv a_1 10 + a_0 (\text{mod } 4) \end{aligned} \tag{2}$$

Thus, if $(10a_1 + a_0) \equiv 0 (\text{mod } 4) \Rightarrow n \equiv 0 (\text{mod } 4)$. Thus, divisibility of n by 4 is decided by the divisibility of $(10a_1 + a_0)$ by 4.

c) We know that $10 \equiv 0 (\text{mod } 5)$, as, 10 is a multiple of 5. Consequently, $10^k \equiv 0 (\text{mod } 5)$, for all $k \geq 1$. Then

$$\begin{aligned} n &\equiv (a_p 10^p + a_{p-1} 10^{p-1} + \ldots + a_0) (\text{mod } 4) \\ &\equiv a_0 (\text{mod } 4) \end{aligned} \tag{3}$$

Thus, if $a_0 \equiv 0 (\text{mod } 5) \Rightarrow n \equiv 0 (\text{mod } 5)$. Thus, divisibility of n by 5 is decided by the divisibility of a_0 by 5. Hence, n is divisible by 5, only if a_0 is equal to 0 or 5.

Exercise 6

a) Let us suppose that n is a number that verifies $n \equiv 3 (\text{mod } 4)$. According to the fundamental theorem of arithmetics, n can be written as the product of prime factors:

$$n = q_1 . q_2 . q_3 . \ldots . q_p$$

where the q_i are prime factors.
Let us divide q_i by 4: there exists k and r with $0 \leq r \leq 3$ such that $q_i = 4k + r$. If $r = 0$ or $r = 2$, q_i would be even, which contradicts that q_i is prime. Therefore $r = 1$ or $r = 3$, i.e. $q_i \equiv 1 (\text{mod } 4)$ or $q_i \equiv 3 (\text{mod } 4)$.
Let us suppose that n has no prime factor that is congruent to 3 modulo 4. Then all q_i would be congruent to 1 modulo 4, and then $n \equiv 1 (\text{mod } 4)$, which contradicts the premise that $n \equiv 3 (\text{mod } 4)$. Therefore the hypothesis "n has no prime factor that is congruent to 3 modulo 4" is false, which can be translated as "n has at least one prime factor that is congruent to 3 modulo 4".

b) Let us suppose that there is a finite set S of prime numbers $\{p_1, p_2, \ldots, p_n\}$ that are congruent to 3 modulo 4. Let us define $n = 4.p_1.p_2 \ldots p_n - 1$. $n \equiv -1 (\mathrm{mod}\ 4)$, i.e. $n \equiv 3 (\mathrm{mod}\ 4)$. Using the result of 6(a), we know that n has at least one prime factor q that is congruent to 3 modulo 4. Since we suppose that the set of prime numbers congruent to 3 modulo 4 is finite, q belongs to S. Therefore q divides $4p_1p_2 \ldots p_n$. Since q is also a divisor of n, q is a divisor of $4p_1p_2 \ldots p_n - n = 1$. Since the only divisor of 1 is 1, this would indicate that $q = 1$, which contradicts q is prime.

The hypothesis that S is finite is false, and therefore there is an infinite number of prime numbers that are congruent to 3 modulo 4.

Part III

Algorithm :

Procedure Replace_with_Preceding_SquareSum($a_1, a_2, \ldots, a_n$, n: Integer)
Integer sum, i, temp ;
sum← $a_1 * a_1$;
for (i = 2 ; i≤ n ; STEP=1)
    temp ← a_i ;
    a_i ← sum ;
    sum ← sum + temp * temp ;
endfor

The complexity of this algorithm is $O(n)$. Each step in the FOR loop requires 1 comparison, 3 assignments, two additions (including the addition for the index i) and one multiplication. Since there are $(n-1)$ steps, this yields $(n-1)$ comparisons, $3(n-1)$ assignments, $2(n-1)$ additions, and $(n-1)$ multiplications, to which we must add 1 multiplication and 1 addition for initializing S. The total number of operations is therefore of order n.