CSCA67 - Discrete Mathematics

Instructors:

|	**Dr. Anna Bretscher**	**Dr. Richard Pancer**
Email:	bretscher@utsc.utoronto.ca	pancer@utsc.utoronto.ca
Office:	IC493	IC490
Office Hours:	Monday 12:10 - 1:30	Monday 11:10 - 12:30
	Wednesday 1:10 - 2:00	Friday 1:30 - 3:00
	Friday 1:10 - 2:00 (will change after week 6)	

Question 1.

Part (a) Each option below is a predicate formula. Circle all answers equivalent to the given.
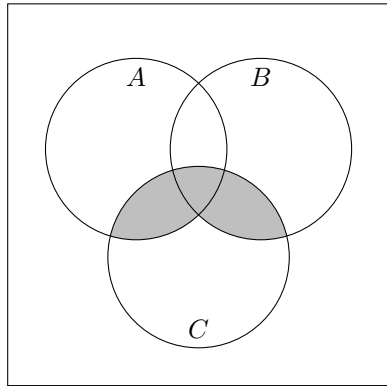
(a) $a \wedge b \wedge c$
(b) $(a \wedge c) \vee (b \wedge c)$
(c) $(\neg b \rightarrow a) \wedge c$
(d) $c \wedge (b \vee a)$
(e) None

Part (b) Write a propositional statement using $\rightarrow$ and $\neg$ if neccesary equivalent to regions 3, 5, and 6. marks you can leave your solution using $\wedge, \vee, \neg$ and $\rightarrow$. You do not need to specify which equivalence laws you use if you need them.
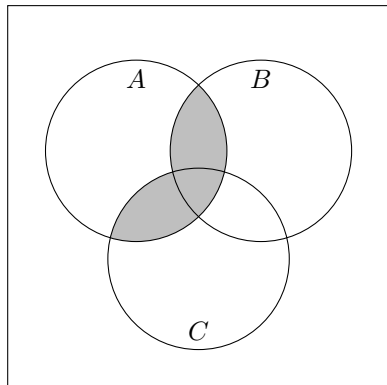
$(a \wedge b) \vee (a \wedge c)$

$a \wedge r(b \vee c)$

$\neg(a \rightarrow \neg(\neg b \rightarrow c))$

Part (c) Circle (I just bolded.) every statement equivalent to $\neg a \rightarrow b$.

(a) $\neg b \rightarrow a$ **(f)** a is neccesary for $\neg b$

(b) $a \rightarrow \neg b$ (g) $\neg a$ is neccesary for b

(c) a is sufficient for $\neg b$ **(h)** b if $\neg a$

(d) $\neg(a \wedge \neg b)$ **(i)** $b \vee a$

(e) b is sufficient for $\neg a$

Question 2.
Determine whether $\forall$ can be factored from an implication. In other words is
$$\forall x \in X, (p(x) \to q(x)) \iff \forall x \in X, p(x) \to \forall x \in X, q(x)$$
true? Explain your reasoning. Marks will only be given for your explanation.

No.
let $p(x) = x > 5$ and $q(x) = x^2 > 25$
$$\forall x \in \mathbb{Z}, (p(x) \to q(x)) \iff \forall x \in \mathbb{Z}, (x > 5 \to x^2 > 25)$$
which means: for all integers x, if x is greater than 5, then x^2 is greater than 5.
vs.
$$\forall x \in \mathbb{Z}, p(x) \to \forall x \in \mathbb{Z}, q(x) \iff \forall x \in \mathbb{Z}, x > 5 \to \forall x \in \mathbb{Z}, x^2 > 25$$
which means: if all integers are greater than 5, then all integers squared are greater than 25.

Sometimes, factoring in $\forall$ can lead to a statment that is true, but never equivalent.
$\forall x \in X, (p(x) \to q(x))$ is saying for every x, if predicate p is true, then predicate q is true.
$\forall x \in X, p(x) \to \forall x \in X, q(x)$ is saying for every x, if predicate p is true, then for every x, predicate q is true, since are not equivalent, therefore $\forall$ cannot be factored into or from an implication.

Question 3.
Answer the following questions to construct a direct proof that:
$$\forall n \in \mathbb{N}, n \geq 2, \forall a, b \in \mathbb{N}, a \equiv_n b \to a^2 \equiv_n b^2$$
Part (a)
Write a and b in terms of n using the division theorem and taking into consideration any common variables.

$$a = k_1 \cdot n + r$$
$$b = k_2 \cdot n + r$$
$$k_1, k_2 \in \mathbb{Z}, r \in [0, (n-1)]$$

Part (b)
Now complete the proof.
Assume $a \equiv_n b$, then that means:

$$a = k_1 \cdot n + r \qquad a^2 = {k_1}^2 \cdot n^2 + 2k_1 \cdot n + r^2$$
$$b = k_2 \cdot n + r \qquad b^2 = {k_2}^2 \cdot n^2 + 2k_2 \cdot n + r^2$$
$$\underline{k_1, k_2 \in \mathbb{Z}, r \in [0, (n-1)]}$$

$$a^2 = {k_1}^2 \cdot n^2 + 2k_1 \cdot n + r^2 = n({k_1}^2 \cdot n + 2k_1) + r^2$$

$$b^2 = {k_2}^2 \cdot n^2 + 2k_2 \cdot n + r^2 = n({k_2}^2 \cdot n + 2k_2) + r^2$$

Since both a^2 and b^2 share the same remainder r^2 when divided by n,
$\therefore \forall n \in \mathbb{N}, n \geq 2, \forall a, b \in \mathbb{N}, a \equiv_n b \to a^2 \equiv_n b^2$. $\qquad\qquad QED$

Question 4.
Prove that $\forall n \in \mathbb{N}, (n^2 - 1 \not\equiv_4 0) \rightarrow n$ is even.

Assume the contrapositive
$n \in \{2k+1\}, k \in \mathbb{Z} \rightarrow (n^2 - 1 \equiv_4 0)$

$$
\begin{aligned}
&n = 2k + 1, k \in \mathbb{Z} \\
&n^2 = 4k^2 + 4k + 1 \\
&n^2 - 1 = 4k^2 + 4 = 4(k^2 + 1) \\
&n^2 - 1 \equiv_4 0
\end{aligned}
$$

Since we prove the contrapositive to be true, and the contrapositive is logically equivalent to the original,
$\therefore n \in \{2k+1\}, k \in \mathbb{Z} \rightarrow (n^2 - 1 \equiv_4 0)$ $\hspace{2cm} QED$