Math 307, Midterm Exam 1
Fall 2024
Instructor: Ostrik

Name: ______________________________

Instructions: You can use a notecard. No calculators are allowed. Common tautologies which we use often (e.g., DeMorgan's Laws) can be used without giving truth tables; more complicated tautologies need to be verified. This is a 50 minute exam.

1. (10 points) Show that $P \Rightarrow R, \sim R, V \Rightarrow (P \vee \sim Q) \vdash V \Rightarrow \sim Q$. Give a two-column logic proof with steps and justifications.

   Proof:

	Statement	Explanation
1.	$P \Rightarrow R$	hyp.
2.	$\sim R$	hyp.
3.	$V \Rightarrow (P \vee \sim Q)$	hyp.
4.	V	dischargeable hyp.
5.	$(P \vee \sim Q)$	MP, For 3, For 4
6.	$\sim P$	MT, For 1, For 2
7.	$\sim Q$	DI, For 5, For 6
8.	$V \Rightarrow \sim Q$	DT, discharge For 4, (4)–(7) unusable

2. (14 points)

(a) (7 points) Solve the equation $(2 \cdot_{13} x) +_{13} 7 = 2$ in $\mathbb{Z}_{13}$. Show all of your steps.

Solution: The additive inverse of 7 in $\mathbb{Z}_{13}$ is 6 and the multiplicative inverse of 2 in $\mathbb{Z}_{13}$ is 7. Hence

$$(2 \cdot_{13} x) +_{13} 7 = 2$$

$$2 \cdot_{13} x = (2 \cdot_{13} x) +_{13} (7 +_{13} 6) = ((2 \cdot_{13} x) +_{13} 7) +_{13} 6 = 2 +_{13} 6 = 8$$

$$x = (7 \cdot_{13} 2) \cdot_{13} x = 7 \cdot_{13} (2 \cdot_{13} x) = 7 \cdot_{13} 8 = 4$$

Check: $(2 \cdot_{13} 4) +_{13} 7 = 8 +_{13} 7 = 2$.

Answer: $x = 4$.

(b) (7 points) Find the multiplicative inverse of 30 in $\mathbb{Z}_{133}$.

Solution: Let us run the Euclidean algorithm:

$$133 = 4 \cdot 30 + 13; \; 30 = 2 \cdot 13 + 4, \; 13 = 3 \cdot 4 + 1.$$

Backwards:

$$1 = 13 - 3 \cdot 4 = 13 - 3 \cdot (30 - 2 \cdot 13) = 7 \cdot 13 - 3 \cdot 30 = 7 \cdot (133 - 4 \cdot 30) - 3 \cdot 30 = 7 \cdot 133 - 31 \cdot 30.$$

Hence

$$1 \equiv -31 \cdot 30 \equiv (133 - 31) \cdot 30 \equiv 102 \cdot 30 \pmod{133}$$

Answer: the multiplicative inverse of 30 in $\mathbb{Z}_{133}$ is 102.

3. (10 points) Given $\sim P \Rightarrow [T \vee S]$, $T \Rightarrow R$, $\sim S$, prove $P \vee R$. Give a two-column logic proof with steps and justifications. Hint: Use proof by contradiction.

Proof:

	Statement	Explanation
1.	$\sim P \Rightarrow [T \vee S]$	hyp.
2.	$T \Rightarrow R$	hyp.
3.	$\sim S$	hyp.
4.	$\sim(P \vee R)$	dischargeable hyp.
5.	$\sim(P \vee R) \Leftrightarrow (\sim P \wedge \sim R)$	taut., de Morgan
6.	$\sim P \wedge \sim R$	MPB, For 5, For 4
7.	$\sim P$	LCS, For 6
8.	$T \vee S$	MP, For 1, For 7
9.	$\sim R$	RCS, For 6
10.	$\sim T$	MT, For 2, For 9
11.	S	DI, For 8, For 10
12.	$S \wedge \sim S$	CI, For 11, For 3
13.	$P \vee R$	II, discharge For 4, (4)–(12) unusable

4. (5 points) Translate the following English sentence into mathematical notation: "Every integer (strictly) larger than 1000 is either a multiple of two or a multiple of three or both."

Answer: $(\forall x)[(x \in \mathbb{Z} \wedge x > 1000) \Rightarrow (2|x \vee 3|x)]$.

5. (5 points) Let $S = \{x \in \mathbb{Z} \,|\, x \geq 13 \wedge (\exists y)[y \in \mathbb{N} \wedge x = 70 - y^3]\}$. Identify the set S by listing all of its elements.

Answer: $S = \{43, 62, 69\}$.

6. (6 points) Determine whether or not the proposition $[(P \vee R) \wedge (P \Rightarrow R)] \Rightarrow P$ is a tautology, by completing the truth table below:

P	R	$P \vee R$	$P \Rightarrow R$	$(P \vee R) \wedge (P \Rightarrow R)$	$[(P \vee R) \wedge (P \Rightarrow R)] \Rightarrow P$
T	T	T	T	T	T
T	F	T	F	F	T
F	T	T	T	T	F
F	F	F	T	F	T

Is the given proposition a tautology? No, this is not a tautology.

7. (10 points) Give a line proof that $(\forall a, b)[(a, b \in \mathbb{Z} \wedge a \equiv_4 2 \wedge 6|b) \Rightarrow 2|a-b]$.

Proof:

1.	Assume $a, b \in \mathbb{Z}$, $a \equiv_4 2$, and $6\|b$	dis. hyp.
2.	$6\|b$	
3.	$b = 6k$ for some k in $\mathbb{Z}$	IE
4.	$a \equiv_4 2$	
5.	$4\|a-2$	
6.	$a - 2 = 4l$ for some l in $\mathbb{Z}$	IE
7.	$a = 4l + 2$	
8.	$a - b = (4l + 2) - 6k = 2 \cdot (2l + 1 - 3k)$	
9.	$(\exists r)[r \in \mathbb{Z} \wedge a - b = 2r]$	EI
10.	$2\|a-b$	
11.	$(a, b \in \mathbb{Z} \wedge a \equiv_4 2 \wedge 6\|b) \Rightarrow 2\|a-b$	DT, discharge For 1, (1)–(10) unusable
12.	$(\forall a, b)[(a, b \in \mathbb{Z} \wedge a \equiv_4 2 \wedge 6\|b) \Rightarrow 2\|a-b]$	IU