MATH 307 SPRING 2025
WEEK 4 HOMEWORK
DUE APRIL 28

INSTRUCTOR: ROBERT LIPSHITZ

Note on your solutions who you worked with, anyone else you got help from, and any materials other than the textbooks that you used. *Electronic resources (Google, ChatGPT, Chegg, etc.) except the textbooks are* ***not*** *allowed. Note*: Updated slightly on April 22.

Required problems (turn these in):

(1) Copy the following onto your own paper and fill in the blanks to prove that addition on $\mathbb{Z}/n$ is commutative. Here, we will let $+$ denote addition in $\mathbb{Z}$, and $\oplus$ addition in $\mathbb{Z}/n$.

(1)	Suppose $x, y \in \mathbb{Z}/n$	Hyp for DT
(2)	$(x + y \geq n) \vee (x + y < n)$	
(3)	Suppose $x + y \geq n$	$\boxed{\quad}$
(4)	$x \oplus y = x + y - n$	Def $\oplus$ (using (3))
(5)	$x + y = y + x$	Algebra ($+$ on $\mathbb{Z}$ commutative)
(6)	$y + x > n$	
(7)	$y \oplus x = y + x - n$	$\boxed{\quad}$
(8)	$y \oplus x = x + y - n$	Property of equality (7), (5)
(9)	$y \oplus x = x \oplus y$	Property of equality (4), (8)
(10)	$(x + y \geq n) \Rightarrow (x \oplus y = y \oplus x)$	$\boxed{\quad}$
(11)	$\boxed{\quad}$	Hyp for DT
(12)	$\boxed{\quad}$	Def $\oplus$ (using (11))
(13)	$y + x = x + y$	Algebra ($+$ on $\mathbb{Z}$ commutative)
(14)	$y + x < n$	
(15)	$y \oplus x = y + x$	
(16)	$y \oplus x = x + y$	Property of equality (15, 13)
(17)	$x \oplus y = y \oplus x$	Property of equality (16, 12)
(18)	$\boxed{\quad}$	DT for Hyp (11), (11)–(17) unusabl
(19)	$[(x + y \geq n) \vee (x + y < n)] \Rightarrow (y \oplus x = x \oplus y)$	$\boxed{\quad}$
(20)	$(\forall a)(\forall b)[(a \in \mathbb{Z} \wedge b \in \mathbb{Z}) \Rightarrow (a + b \geq n \vee a + b < n)]$	algebra (trichotomy)
(21)	$\boxed{\quad}$	US (20)
(22)	$x \oplus y = y \oplus x$	MP (18), (21)
(23)	$\boxed{\quad}$	DT for Hyp (1)
(24)	$(\forall x)(\forall y)[(x \in \mathbb{Z}/n \wedge y \in \mathbb{Z}/n) \Rightarrow (x \oplus y = y \oplus x)]$	$\boxed{\quad}$

(2) Fill in the blanks in the outline below to prove that $(\forall n)[(n \in \mathbb{N} \wedge 3 \nmid n) \Rightarrow n^2 \equiv_3 1]$. Also:

- (b) There are three uses of the Deduction Theorem in this proof. Label the appropriate DT steps (both the hypotheses and where DT is applied).
- (b) There are two steps at the end of the proof with the phrase "Logical rule?" in bold. For these, label the appropriate rule from symbolic logic that is being used.

(1) Assume $\boxed{}$

(2) $n \not\equiv_3 0$

(3) So either $n \equiv_3 1$ or $n \equiv_3 2$

(4) Assume $n \equiv_3 1$.

(5) Then $3 | \boxed{}$

(6) So $n - 1 = 3 \cdot P$ for some $\boxed{}$

(7) $n = \boxed{}$

(8) $n^2 = \boxed{} = 3 \cdot \boxed{} + 1$

(9) $n^2 - 1 = \boxed{}$

(10) $(\exists y)[y \in \mathbb{Z} \wedge \boxed{}]$

(11) $3 | \boxed{}$

(12) $n^2 \equiv_3 1$

(13) So $n \equiv_3 1 \Rightarrow n^2 \equiv_3 1$.

(14) Now assume $n \equiv_3 2$.

(15) $\boxed{}$

(16) $\boxed{}$

(17) $\boxed{}$

(18) $\boxed{}$

(19) $\boxed{}$

(20) $\boxed{}$

(21) $\boxed{}$

(22) $\boxed{}$

(23) So $n \equiv_3 2 \Rightarrow n^2 \equiv_3 1$.

(24) We therefore have $(n \equiv_3 1 \vee n \equiv_3 2) \Rightarrow n^2 \equiv_3 1$ **Logical rule?**

(25) So $n^2 \equiv_3 1$ **Logical rule?**

(26) $(n \in \mathbb{N} \wedge 3 \nmid n) \Rightarrow n^2 \equiv_3 1$

(27) $\boxed{}$

(3) Give a proof, in the same style as the previous problem, of: $(\forall n)[(n \in \mathbb{N} \wedge n \equiv_6 3) \Rightarrow n^2 + 2n + 10 \equiv_{12} 1]$.

(4) The most common way to prove a statement of the form $(\exists x)[P(x)]$ is to produce an explicit example of an x for which $P(x)$ is true. For example, to prove

$$(\exists n)[n \in \mathbb{N} \wedge 3|(n^2 + 2n)]$$

we can simply say "4 is a natural number, $4^2 + 2 \cdot 4 = 24$, and $3|24$." This is called *giving an example.*

The negation of $(\forall x)[P(x)]$ is $(\exists x)[\neg P(x)]$. Disproving the former statement is the same as proving the latter statement. So applying the above principle, if we want to disprove a "for all" statement then we should try to produce an explicit x such that $\neg P(x)$ is true. This is called *giving a counterexample.*

For instance: we can disprove the statement

$$(\forall n)[n \in \mathbb{Z} \Rightarrow 3|n^2 + 2n]$$

simply by saying "5 is in $\mathbb{Z}$, $5^2 + 2 \cdot 5 = 35$, and $3 \nmid 35$". (Note that we are disproving $P \Rightarrow Q$ by proving $P \wedge \neg Q$.)

Identify each of the following statements as true or false. Where you can, prove the statement by giving an example or disprove it by giving a counterexample.

(a) $(\exists x)[x \in \mathbb{Z}/9 \wedge x^2 \in \{5, 7\}]$
(b) $(\forall a)[(a \in \mathbb{Z} \wedge a^2 \equiv_{11} 16) \Rightarrow a \equiv_{11} 4]$
(c) $(\exists n)[n \in \mathbb{N} \wedge \left(\frac{1}{2}(n^2 + n) + 2 \text{ is prime}\right)]$
(d) $(\forall n)[n \in \mathbb{N} \Rightarrow \left(\frac{1}{2}(n^2 + n) + 2 \text{ is prime}\right)]$
(e) $(\exists a, b)(a, b \in \mathbb{Z} \wedge 12a + 20b = 4)$

(5) Use the Euclidean algorithm to find the multiplicative inverse for 24 in $\mathbb{Z}/29$.

(6) Give a three-column proof (skipping some steps if you like) that $(\forall n)[n \in \mathbb{N} \Rightarrow n^2 + (n+1)^2 + (n+2)^2 \equiv_3 2]$.

(7) Exactly one of the following is a ring. For each which is *not* a ring, find an axiom that fails and an example showing that it fails.

(a) $(\mathbb{Z}, -, \times)$, the integers with the operations of subtraction and multiplication.
(b) $(\{a + b\sqrt{2} \in \mathbb{R} \mid a, b \in \mathbb{Z}\}, +, \times)$, where $+$ and $\times$ are the usual addition and multiplication on $\mathbb{R}$.
(c) $(\{x \in \mathbb{R} \mid x \geq 0\}, +, \times)$, where $+$ and $\times$ are the usual addition and multiplication on $\mathbb{R}$.
(d) $(\mathbb{Q}/\mathbb{Z}, \oplus, \times)$ where $\mathbb{Q}/\mathbb{Z}$ means the rational numbers p/q with $0 \leq \frac{p}{q} \leq 1$, with the usual multiplication and with addition given by

$$\frac{p}{q} \oplus \frac{r}{s} = \begin{cases} \frac{p}{q} + \frac{r}{s} & \text{if } \frac{p}{q} + \frac{r}{s} < 1 \\ \frac{p}{q} + \frac{r}{s} - 1 & \text{if } 1 \leq \frac{p}{q} + \frac{r}{s} < 2 \\ 0 & \text{if } \frac{p}{q} + \frac{r}{s} = 2. \end{cases}$$

(8) Here is an important property of prime numbers. If p is prime, then

$$\text{Property (P)}: \qquad (\forall x, y \in \mathbb{Z})[p|xy \Rightarrow (p|x \vee p|y)].$$

Using this, fill in the blanks below to give a proof of the following theorem:
Theorem: $(\forall y)[(y \in \mathbb{Z} \wedge 4y^2 \equiv_7 0) \Rightarrow y \equiv_7 0]$

Proof:

(1) Assume $y \in \mathbb{Z}$ and $4y^2 \equiv_7 0$.
(2) Then $\boxed{\quad}$.
(3) 7 is prime, so by property (P) we know $7|4$ or $\boxed{\quad}$.
(4) But $7 \nmid 4$, so $\boxed{\quad}$.
(5) Using Property (P) again, either $7|y$ or $\boxed{\quad}$.
(6) Therefore $7|y$ (by using the tautology $\boxed{\quad}$).
(7) $\boxed{\quad}$.
(8) $\boxed{\quad}$.
(9) $\boxed{\quad}$.

(9) Give a proof that $(\forall n)[(n \in \mathbb{N} \wedge 3|n \wedge n \equiv_5 3) \Rightarrow n^2 + n \equiv_{15} 12]$.
Hint: you will need Property (P) at some point of your proof.

(10) Provisionally, a *rational number* is a number of the form $\frac{a}{b}$ where $a, b \in \mathbb{Z}$ and $b \neq 0$. As you learned in elementary school, a rational number can always be written in the form where $\gcd(a, b) = 1$. Fill in the blanks below to give a proof of the following theorem; feel free to insert extra steps if you think it will help clarify the proof.
Theorem: $\sqrt{2}$ is not a rational number.

(1) Assume that $\sqrt{2}$ is a rational number.
(2) Then $\sqrt{2} = \frac{a}{b}$ for some $a, b \in \mathbb{Z}$ where $b \neq 0$ and $\gcd(a, b) = 1$.
(3) So $2 = \frac{a^2}{b^2}$, and therefore $a^2 = \boxed{\quad}$.
(4) So $2|a^2$.
(5) Then by Property (P), $\boxed{\quad}$.
(6) $a = 2r$ for some $r \in \mathbb{Z}$.
(7) $2b^2 = \boxed{\quad}$.
(8) $b^2 = \boxed{\quad}$.
(9) $2|b^2$
(10) So using Property (P), $\boxed{\quad}$.
(11) $b = 2s$ for some $s \in \mathbb{Z}$.
(12) This is a contradiction, because $\boxed{\quad}$.
(13) $\boxed{\quad}$.

(11) Give a similar proof that $\sqrt{10}$ is not a rational number.

Extra Practice. Do not turn these in, but if you had trouble with some of the required arguments, here are some more to practice, for which I will post solutions.

(EP-0) Give a proof, in the style of Problem 2, that:

$$(\forall n)[(n \in \mathbb{N} \wedge n \equiv_5 2) \Rightarrow (2 \nmid n \vee n^2 \equiv_{20} 4)]$$

[Hint: Remember that $(X \vee Y) \Leftrightarrow (\neg X \Rightarrow Y)$. Use DT twice in this proof.]

(EP-0) Identify each of the following statements as true or false. Where you can, prove the statement by giving an example or disprove it by giving a counterexample.

(a) $\{x \mid x \in \mathbb{Z}/8 \wedge 4 \cdot_8 x = 0\} \cap \{4 \cdot_8 x \mid x \in \mathbb{Z}/8\} = \emptyset$

(b) $(\forall n)[(n \in \mathbb{N} \wedge n \equiv_2 1 \wedge n > 3) \Rightarrow 3|n^2 - 1]$

(c) $(\forall a, b)[(a, b \in \mathbb{Z} \wedge 12|ab) \Rightarrow (12|a \vee 12|b)]$

(EP-0) Decide if the following statement is true or false. If it is true, give a three-column proof. If it is false, give a counterexample:

$$(\forall a, b, c)\big[(a, b, c \in \mathbb{Z} \wedge a > 0 \wedge a|(b-1) \wedge a|(c-1)\,) \Rightarrow a|(bc-1)\big].$$

Email address: `lipshitz@uoregon.edu`