MATH 307 SPRING 2025
WEEK 5 HOMEWORK
DUE MAY 5

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.*

Required problems (turn these in):

(1) Fill in the boxes in the following proof that, in a ring, $(\forall a)(\forall b)[-(a+b) = (-a) + (-b)]$.

(1)	$a + (-a) = 0$	Definition of additive inverse
(2)	$b + (-b) = 0$	Definition of additive inverse
(3)	$0 + 0 = 0$	
(4)	$(a + (-a)) + 0 = 0$	Substitution (1) into (3)
(5)	$(a + (-a)) + (b + (-b)) = 0$	
(6)	$((a + (-a)) + b) + (-b) = 0$	
(7)		
(8)	$(a + (b + (-a))) + (-b) = 0$	
(9)		Axiom (associativity of $+$)
(10)	$(a + b) + ((-a) + (-b)) = 0$	
(11)		Lemma: uniqueness of additive inverses
(12)		

(2) Write the previous proof in paragraph form. (Feel free to merge some of the steps above in your paragraph version.)

(3) Formulate precisely and then give a column proof of the following statement about elements of a ring: If an element has a multiplicative inverse, then its multiplicative inverse is unique.

(4) Give a column proof that there is no way to put an order on $\mathbb{C}$ so that $\mathbb{C}$ becomes an ordered ring. Do this by Indirect Inference: assume there is an order $<$ on $\mathbb{C}$ satisfying the axioms of an ordered ring (with the usual addition and multiplication on $\mathbb{C}$), and derive a contradiction. You may use Problems (EP-2) and (EP-3), and it's okay to skip easy logic steps.

(5) Is it possible to use the ring axioms to prove the following statement? If so, give a proof. If not, explain precisely why not.

$$(\forall x)(\forall y)[\neg(x \times x + y \times y = -1)]$$

(6) Give a paragraph proof of: An integer is divisible by 3 if and only if the sum of its digits (written in base 10) is divisible by 3. (Hint: what does it mean to write a number in base 10?)

(7) What is the analogue of the previous problem for divisibility by 9? By 11? By 7? By 37? In each case, explain why your answer is correct *and* give a couple of examples illustrating it.

(8) Suppose p and a are natural numbers and $\gcd(p, a) = 1$ (i.e., p and a are relatively prime). The *multiplicative order of a in $\mathbb{Z}/p$* is the smallest natural number n so that $a^n \equiv 1 \pmod{n}$.
   (a) Compute the multiplicative order of every non-zero element of $\mathbb{Z}/5$ and of every non-zero element of $\mathbb{Z}/7$.
   (b) Compute the multiplicative orders of $1, 3, 5, 7$ in $\mathbb{Z}/8$.
   (c) If p is prime, then Fermat's Little Theorem gives an upper bound on the multiplicative orders of elements of $\mathbb{Z}/p$. What is it?

(9) Fill in the following proof that: If p is a prime and $a \in \mathbb{Z}/p$ has multiplicative order $p-1$, then any non-zero element of $\mathbb{Z}/p$ is equal to a^k for some k.

First, we show that for all k, $a^k \neq 0$ (in $\mathbb{Z}/p$). So, suppose that _____. (That is, we are arguing by _____.) If $a^k = 0$ in $\mathbb{Z}/p$, then _____. So, $p|a(a^{k-1})$. By _____, either $p|a$ or $p|a^{k-1}$. Repeating this argument with a^{k-1} in place of a^k, we eventually see that $p|a$. But then _____, so _____. Thus, $a^k \neq 0$.

Now, since $\mathbb{Z}/p$ has p many elements and we showed 0 is not a power of a, it suffices to show that $\{a, a^2, a^3, \dots, a^{p-1}\} \subset \mathbb{Z}/p$ has exactly _____ many elements. So, suppose that _____. (We are again using _____.) Then $a^m = a^n$ for some $1 \leq m < n \leq p-1$. Multiplying both sides by _____ gives _____. But this implies that the order of a is at most _____. Since, by hypothesis, the order of a is _____, this is a contradiction. Hence, _____ has _____ many elements and so $\{a, a^2, \dots, a^{p-1}\} =$ _____, proving the result.

(10) An integer $n > 1$ is a *Carmichael number* if for every $1 \leq a \leq n-1$, $a^n \equiv a \pmod{n}$. Give a paragraph proof that there are no even Carmichael numbers. (Hint: what special elements of $\mathbb{Z}/n$ can you quickly raise to powers?) (Note: it was only proved in the 1990s that there are infinitely many Carmichael numbers.[1])

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

(EP-0) Recall that $\mathbb{C} = \{a + bi \mid a, b \in \mathbb{R}\}$, with addition given by $(a + bi) + (c + di) = (a+c)+(b+d)i$ and multiplication given by $(a+bi)(c+di) = (ac-bd)+(ad+bc)i$. (More formally, we can view $\mathbb{C}$ as $\mathbb{R}^2$ with addition $(a, b)+(c, d) = (a+c, b+d)$ and multiplication given by $(a, b)(c, d) = (ac - bd, ad + bc)$. When we write elements of $\mathbb{C}$ as $a+bi$, i and the plus sign are place-holders, like the comma in an ordered pair.) Assuming that we already know $\mathbb{R}$ is a ring, check that $\mathbb{C}$ is a ring and, in fact, a field. (You have 9 properties to check, but they're all quick. You don't have to be

[1] W. R. Alford, Andrew Granville and Carl Pomerance, "There are Infinitely Many Carmichael Numbers." *Annals of Mathematics* Vol. 139, No. 3 (May, 1994), pp. 703-722.

careful about parenthesizing products of real numbers—apply associativity for real numbers as much as you like. And, I'm not asking for column proofs here.)

(EP-0) Give a column proof: in an ordered ring R, $a < 0 \Leftrightarrow 0 < (-a)$.

(EP-0) Give a column proof: in a nontrivial ordered ring R, $0 < 1$.

(EP-0) Prove: In the ring $\mathbb{Z}/3$, $(x+y)^3 = x^3 + y^3$. What is the analogous statement over $\mathbb{Z}/2$? Over $\mathbb{Z}/5$?

(EP-0) Turn the statement proved in Problem (9) into a formula (with quantifiers and so on).

(EP-0) Suppose that $n = m^2 k$ for some natural numbers m and k with $m > 1$. Prove that n is not a Carmichael number. Also, why did I have to include the assumption that $m > 1$?

(EP-0) Given prime numbers p and q, define $\left(\frac{p}{q}\right)$ to be 1 if p is as square modulo q and -1 if p is not a square modulo q.

(a) What is $\left(\frac{7}{11}\right)$? $\left(\frac{11}{7}\right)$? $\left(\frac{5}{11}\right)$? $\left(\frac{11}{5}\right)$? $\left(\frac{5}{13}\right)$? $\left(\frac{13}{5}\right)$?

(b) Gauss's famous *Quadratic Reciprocity Theorem* says that

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}.$$

Verify that Quadratic Reciprocity held in the examples above, and use it to determine if 113 is a square modulo 257.

Email address: lipshitz@uoregon.edu