

MathTLC Algebra & Number Theory
Understandings Exam
Summer 2009

Instructions: Answer each of the following questions. **Show all your work.** You can use your notes and the lecture material. General discussions of topics related to the exam are permitted. Discussions about individual problems are not allowed. Use of web resources such as AskJeeves is prohibited. If you have questions about the problems, please correspond with me.

Remember: perspiration, desperation and inspiration; these problems will look scary at first, but you can do them!

The exam is due by 11:59 p.m. on Friday, July 24.

1. This problem concerns the binary structure given by the following table

\circ	a	b	c	d
a	b	a	c	d
b	a	b	c	d
c	d	c	c	d
d				

- (a) Complete the table so that \circ is associative. (There is only one way. Make sure to explain how you arrive at your answer.)
- (b) Is \circ commutative?
2. It is known that the product of the two integers

$$m = 43143047130174\mathbf{y}3091873027410479407$$

and

$$n = 13243473089471321230233043091734$$

is

$$57136378366625534110287200887739529349648747833611258918418921738$$

where \mathbf{y} represents an unknown digit.

- (a) Use mod 9 arithmetic to show that $7(y + 1) \equiv 3 \pmod{9}$.
- (b) Solve the equation in (a) by using valid mod arithmetic rules (e.g. you can't divide!)
3. In this problem, we will establish a divisibility-by-7 criteria. Let n be an integer with decimal representation $d_k d_{k-1} \cdots d_2 d_1 d_0$. Let m be the integer with decimal representation $d_k d_{k-1} \cdots d_2 d_1$.
- (a) Explain why $n = 10m + d_0$.
- (b) Explain why $n \equiv 0 \pmod{7}$ if and only if $3m + d_0 \equiv 0 \pmod{7}$.
- (c) Explain why $3m + d \equiv 0 \pmod{7}$ if and only if $m - 2d_0 \equiv 0 \pmod{7}$. (Hint: Multiply by through by 5.)
- (d) Use (a)-(c) to explain why 7 divides n if and only if 7 divides $m - 2d_0$.

- (e) Repeatedly use (d) to decide whether or not 623413 is a multiple of 7. (You stop, once you get to a 2-digit number.)
4. This problem concerns a modified version of the Division Algorithm when one is dividing by 7. We wish to show that for each positive integer a there exists integers q and r such that $a = 7q + r$ and $-3 \leq r \leq 3$.
- Find such q and r for $a = 11$
 - Use your answer in (a) to find such q and r for $a = 18$.
 - Explain how the idea in (a) and (b) can be generalized to reduce the problem of finding such q and r for any integer $a \geq 8$ to a “smaller” problem.
 - Prove that for each positive integer a , the q and r are unique.
5. This problem concerns the Gaussian integers.
- Show that $7 + 4i$ is not irreducible, by expressing it as a product of two non-units. (Hint: If $7 + 4i = uv$, then $N(u)N(v) = 65$. So you should be searching for a factor u with $N(u) = 5$).
 - Express $105 + 60i$ as a product of irreducibles in $\mathbb{Z}[i]$. (Make sure that you justify why each claimed factor is irreducible.)
6. This problem concerns functions $f : \mathbb{Z}_{15} \rightarrow \mathbb{Z}_{15}$.
- Show that the function $f : \mathbb{Z}_{15} \rightarrow \mathbb{Z}_{15}$ defined by $f(x) = 3x + 5$ is not a one-to-one function.
 - Show that the function $g : \mathbb{Z}_{15} \rightarrow \mathbb{Z}_{15}$ defined by $g(x) = 2x - 7$ is onto by solving $2x - 7 = y$ (over \mathbb{Z}_{15}) for an arbitrary y . (Remember in mod arithmetic you can't divide!)
 - Explain why g is also one-to-one.
 - By (b) and (c), g is a permutation of \mathbb{Z}_{15} . Express g as a product of disjoint cycles.
7. This problem concerns the Quadratic Formula over the field of integers mod p , where p is a prime and $p \neq 2$. We will stick to $p = 7$ for simplicity.
- Let's start easy, by solving $x^2 - 4$ over \mathbb{Z}_7 . Use factoring and the fact that \mathbb{Z}_7 is a field to show that the only solutions are $x = 2$ and $x = -2 = 5$.
 - Now let's solve $x^2 - 2$ over \mathbb{Z}_7 by using the fact that $2 = 3^2$ in \mathbb{Z}_7 .
 - Next show that $x^2 - 3$ over \mathbb{Z}_7 has no solutions, since 3 is not a perfect square in \mathbb{Z}_7 .
 - Next solve $x^2 + 4x + 2 = 0$ over \mathbb{Z}_7 by completing the square and reducing the problem to $(x+2)^2 + 2 - 4 = 0$.
 - Now show that $x^2 + 4x + 1 = 0$ over \mathbb{Z}_7 has no solutions by completing the square.
 - Next solve $x^2 + 3x + 2 = 0$ over \mathbb{Z}_7 by the method of completing squares (and noting that $3 = 2 \cdot 5$ here).
 - Step this up a notch and use the completing the square process to solve $4x^2 + 3x + 6 = 0$ in \mathbb{Z}_7 (Hint: First show that $4x^2 + 3x + 6 = 4(x^2 + ux + v)$ for some u and v).
 - (Optional challenge problem: The quadratic formula for \mathbb{Z}_7)
Use the completing the squares method to show that if $a \neq 0$, then over \mathbb{Z}_7 the equation $ax^2 + bx + c = 0$ has no solutions if $b^2 - 4ac$ is not a perfect square, and otherwise the solutions are $(2a)^{-1}(-b \pm d)$ where $d^2 = b^2 - 4ac$.