Name ____ Test 2, Fall 2021

Part 1: Basic Knowledge

1) Let a an element of $\mathbb{Z}_n$. What does it means for a to be invertible? Precisely state the definition. (5 points)

a is invertible if there is some $b \in \mathbb{Z}_n$ such that $ab \equiv 1$.

2) What is a power series? Give an expression for an arbitrary element of $\mathbb{R}[\![x]\!]$. (5 points)

$$\sum_{k=0}^{\infty} a_k x^k$$

3) Let $\otimes$ be a binary operation on a set S. What does it mean for S to be commutative? Precisely state the definition. (5 points)

$$a \otimes b = b \otimes a \text{ for all } a, b \in S$$

4) Consider multiplication in $\mathbb{Z}_n$. What does it mean for multiplication to be well defined? Precisely state the definition. (5 points)

Multiplication is well defined if for all $a_1, a_2, b_1, b_2 \in \mathbb{Z}_n$:

If $a_1 \equiv a_2$ and $b_1 \equiv b_2$, then $a_1 b_1 \equiv a_2 b_2$.

Name ____ Test 2, Fall 2021

Part 2: Basic Skills and Concepts

5) Find the product below, express your answer using the sum-of-degree method. (5 points)

$$\left(\sum_{k=0}^{\infty} 2^k x^k\right)\left(\sum_{k=0}^{\infty} 3^k x^k\right)$$

$$\sum_{d=0}^{\infty}\sum_{l=0}^{d} 2^l 3^{d-l} x^d$$

6) Find the multiplicative inverse of $\sum_{k=0}^{\infty} \frac{2^k x^k}{k!}$. (5 points)

Note that $\sum_{k=0}^{\infty} \frac{2^k x^k}{k!} = e^{2x}$, which has multiplicative inverse $e^{-2x} = \sum_{k=0}^{\infty} \frac{(-2)^k x^k}{k!}$

7) Find 4^{-1} mod 11. (5 points)

3

8) Below is a derivation of the quadratic formula. It does not work in $\mathbb{Z}_n$. Which is the first step that is not guaranteed to work in $\mathbb{Z}_n$ and why? (5 points)

$ax^2 + bx + c = 0$

$\left(\sqrt{a}x + \frac{b}{2\sqrt{a}}\right)^2 + c - \frac{b^2}{4a} = 0$ This line for one of four reasons:

- We might not be able to divide by 2.
- We might not be able to divide by 4.
- We might not be able to divide by a.
- We might not be able to define $\sqrt{a}$.

$\left(\sqrt{a}x + \frac{b}{2\sqrt{a}}\right)^2 = \frac{b^2}{4a} - c$

$\left(\sqrt{a}x + \frac{b}{2\sqrt{a}}\right)^2 = \frac{b^2-4ac}{4a}$

$\sqrt{a}x + \frac{b}{2\sqrt{a}} = \frac{\pm\sqrt{b^2-4ac}}{2\sqrt{a}}$

$\sqrt{a}x = -\frac{b}{2\sqrt{a}} \pm \frac{\sqrt{b^2-4ac}}{2\sqrt{a}}$

$x = -\frac{b}{2a} \pm \frac{\sqrt{b^2-4ac}}{2a}$

$x = \frac{-b\pm\sqrt{b^2-4ac}}{2a}$

9) Solve $AX + X = B$ for X. Assume the needed inverse exists. (5 points)

$(A + I)X = B$
$X = (A + I)^{-1}B$

10) Find $2 \otimes 1$, given the binary operation below. (5 points)

$\otimes$	1	2	3
1	1	1	2
2	3	1	1
3	2	3	2

$2 \otimes 1 = 3$

Part 3: Proofs

Do not use any advanced theorems that would create circular logic.

11) Let A and B be invertible matrices in $\mathbb{R}^{n\times n}$. Prove that $(AB)^{-1}$ exists. (15 points)

The inverse is $B^{-1}A^{-1}$ as seen below:

$$(AB)(B^{-1}A^{-1}) = ABB^{-1}A^{-1} = AIA^{-1} = AA^{-1} = I$$

We had a theorem that a right inverse is also a left inverse. Or you just should repeat the process on the left as well.

12) Let S be a set with a binary operation $\otimes$. If $a \otimes e = e \otimes a = a$ and $a \otimes f = f \otimes a = a$ for all $a \in S$, Prove that $e = f$. (15 points)

In $a \otimes e = a$, take $a = f$ to get $f \otimes e = f$.
In $f \otimes a = a$, take $a = e$ to get $f \otimes e = e$.

Combine these two equations together via the transitive property to obtain:
$f = f \otimes e = e$

13) Let R be a ring and $a, b \in R$. Prove that $-(-a) = a$. (15 points)

Proof 1:

We know that $a + (-a) = 0$.

$\therefore \left(a + (-a)\right) + \left(-(-a)\right) = -(-a)$	Add $-(-a)$ to both sides
$\therefore a + \left((-a) + \left(-(-a)\right)\right) = -(-a)$	Associative property
$\therefore a + 0 = -(-a)$	Definition of additive inverse
$\therefore a = -(-a)$	Definition of additive identity

Proof 2:

We know that $0 = 0$.

$\therefore 0 = a + (-a)$	Definition of additive inverse.
$\therefore 0 - (-a) = a + (-a) - (-a)$	Add $-(-a)$ to both sides.
$\therefore -(-a) = a + 0$	Definition of additive inverse.
$\therefore -(-a) = a$	Definition of additive identity.

Proof 3:

$a + (-a) = 0$	Definition of additive inverse.
$-a + a = 0$	Commutative property
$\therefore -(-a) = a$	Definition of additive inverse of $-a$.

14) Let p be prime and $a, b \in \mathbb{Z}_p$. Prove that if $ab \equiv 0$, then either $a \equiv 0$ or $b \equiv 0$. This is called the zero product property. (15 points)

Assume $ab \equiv 0$

$\therefore p \mid ab$	Theorem relating mods and division.
$\therefore p \mid a$ or $p \mid b$	Definition of prime.
$\therefore a \equiv 0$ or $b \equiv 0$.	Theorem relating mods and division.