CS250:	D5: the Commutative Rings, $\mathbf{Z}/m\mathbf{Z}$	10/19/16

As usual, you will join random groups of 4 according to the card you are given. Please work together in your groups to understand and solve the problems on this two-sided sheet. There will be a D5 moodle quiz for you to fill in your answers by Thursday night, 11 p.m.

R_1	$\stackrel{\text{def}}{=}$	$\forall x\, y\, z\, (x + (y + z) \ = \ (x + y) + z)$	$+$ is associative
R_2	$\stackrel{\text{def}}{=}$	$\forall x\, y\, (x + y \ = \ y + x)$	$+$ is commutative
R_3	$\stackrel{\text{def}}{=}$	$0 \neq 1 \ \wedge \ \forall x\, x + 0 = x$	0 is id for $+$
R_4	$\stackrel{\text{def}}{=}$	$\forall x\, \exists y\, x + y = 0$	Additive inverses
R_5	$\stackrel{\text{def}}{=}$	$\forall x\, y\, z\, (x \cdot (y \cdot z) \ = \ (x \cdot y) \cdot z)$	$\cdot$ is associative
R_6	$\stackrel{\text{def}}{=}$	$\forall x\, x \cdot 1 = x$	1 is id for $\cdot$
R_7	$\stackrel{\text{def}}{=}$	$\forall x\, y\, z (x \cdot (y + z) = x \cdot y + x \cdot z) \wedge$ $(y + z) \cdot x = y \cdot x + z \cdot x)$	$+$ distributes over $\cdot$
CR	$\stackrel{\text{def}}{=}$	$\forall x\, y\, (x \cdot y \ = \ y \cdot x)$	$\cdot$ is commutative

Def. A **ring** is a world $W \in \text{World}[\Sigma_{\#\text{thy}}]$ s.t. $W \models R_1 \wedge \cdots \wedge R_7$

Def. A **commutative ring** is a ring that satisfies CR $\mathbf{Z}$, $\mathbf{Q}$, $\mathbf{R}$ are commutative rings. $\mathbf{N}$ is not a ring.

Some other commutative rings: $\mathbf{Z}/m\mathbf{Z}$, $m > 1$

$$|\mathbf{Z}/m\mathbf{Z}| = \{0, 1, \ldots, m-1\}, \quad a + b \stackrel{\text{def}}{=} (a + b)\%m, \quad a \cdot b \stackrel{\text{def}}{=} (a \cdot b)\%m$$

Prop. for all $m > 1$, $\mathbf{Z}/m\mathbf{Z} \models R_1 \wedge \cdots \wedge R_7 \wedge CR$

$|\mathbf{Z}/2\mathbf{Z}| = \{0, 1\}$

$+^{Z/2Z}$	0	1
0	0	1
1	1	0

$\cdot^{Z/2Z}$	0	1
0	0	0
1	0	1

$$F \stackrel{\text{def}}{=} \forall x\, (x \neq 0 \ \rightarrow \ \exists y\, x \cdot y = 1)$$

Def. A **field** is a commutative ring that satisfies F $\mathbf{Q}$, $\mathbf{R}$ are fields

$\mathbf{Z}$ is not a field; $\mathbf{Z}/2\mathbf{Z}$ is a field.

$|\mathbf{Z}/3\mathbf{Z}| = \{0, 1, 2\}$

$+^{Z/3Z}$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$\cdot^{Z/3Z}$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

$\mathbf{Z}/3\mathbf{Z}$ is a field

$+^{Z/4Z}$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$.^{Z/4Z}$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

$\mathbf{Z}/4\mathbf{Z}$ is not a field   Which elements of $\mathbf{Z}/4\mathbf{Z}$ have multiplicative inverses?   1,3

$+^{Z/5Z}$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$.^{Z/5Z}$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

$\mathbf{Z}/5\mathbf{Z}$ is a field

$+^{Z/6Z}$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

$.^{Z/6Z}$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

$\mathbf{Z}/6\mathbf{Z}$ is not a field   Which elements of $\mathbf{Z}/6\mathbf{Z}$ have multiplicative inverses?   1,5

Let $a^{-1}\text{mod } m$ denote the multiplicative inverse of a in $\mathbf{Z}/m\mathbf{Z}$, if it exists.

Compute the following:

1. $2^{-1}\text{mod } 3$
2. $3^{-1}\text{mod } 4$
3. $2^{-1}\text{mod } 5$ $3^{-1}\text{mod } 5$ $4^{-1}\text{mod } 5$
4. $5^{-1}\text{mod } 6$

With what time remains, in your group, try to prove the following:

Shuyang's Thm. If $m > 1$ is a perfect square, then $\mathbf{Z}/m\mathbf{Z}$ is not a field.

Jordan and Rachit's Conjecture If $m > 1$ is not prime, then $\mathbf{Z}/m\mathbf{Z}$ is not a field.