Modular Arithmetic

Let n be a positive integer. Recall the congruent-modulo-n equivalence relation defined on $\mathbb{Z}$ where if $a, b \in \mathbb{Z}$, then a is equivalent to b **iff** n / a-b. In this case we write

$$a \equiv b(modn)$$

and we denoted the equivalence class containing a by [a].

EX If n=3, then: [0] = {. . . , -9, -6, -3, 0, 3, 6, 9, . . . } [1] = {. . . , -8, -5, -2, 1, 4, 7, 10, . . . } [2] = {. . . , -7, -4, -1, 2, 5, 8, 11, . . . }

Notation Let $\frac{\mathbb{Z}}{n\mathbb{Z}}$ denote the set of equivalence classes of the congruent-modulo-n equivalence relation. **EX**

$$\frac{\mathbb{Z}}{3\mathbb{Z}} = [0], [1], [2]$$

$$\frac{\mathbb{Z}}{5\mathbb{Z}} = [0], [1], [2], [3], [4]$$

We can do arithmetic with $\frac{\mathbb{Z}}{n\mathbb{Z}}$ by setting

$$[a] + [b] = [a + b]$$

$$[a][b] = [ab]$$

But are these binary operations well-defined? In other words, do they **not** depend on the representatives we choose to use in [a] and [b]? **EX** Insert later

To show that the addition is well-defined, suppose [a]=[a'] and [b] = [b']. We need to show that

$$[a + b] = [a' + b']$$

But if n|a-a' and n|b-b' then n|(a-a')+(b-b'). Since: $$

$$We also have that n|(a + b) - (a' + b'). In other words,$$

[a+b] = [a'+b'] $$ How might you show that multiplication is well-defined? **Insert stuff here later**

Subtraction in $\mathbb{Z}$ can be used to define subtraction in $\frac{\mathbb{Z}}{n\mathbb{Z}}$:

$$[a] - [b] = [a - b]$$

However, division is problematic in $\mathbb{Z}$, so we have to be careful when talking about division in $\frac{\mathbb{Z}}{n\mathbb{Z}}$. We'll do this by talking about multiply by **reciprocals**.