Situation: Modular Arithmetic
Prepared at UGA
Center for Proficiency in Teaching Mathematics
7/17/2006 - Pawel Nazarewicz

1 Prompt

A group of high school Math Club members was examining the concept of modular arithmetic. They were working in mod 5, and as they were getting the hang of things, a student asked if it's possible to write fractions in mod 5. For example, what is the meaning of the statement below?

$$\frac{3}{4} \mod 5$$

2 Commentary

Does this even make sense? Modulo 5 has only 5 elements: 0, 1, 2, 3, and 4. Anything else is in the same equivalence class as one of those elements. Does it makes sense to define a fraction to be equivalent to one of those 5 elements? What are the different definitions of fractions?

We will explore a situation through which we set up a definition of $\frac{3}{4}$ in modulo 5 and discuss the role of fractions in in Real number system.

Mathematical Focus 1: Modular Arithmetic

Before we can talk about fractions in a certain modulo, we need to understand what it means for $a \cong b \mod c$ (Read: a is congruent to b modulo c).

$$\begin{aligned} a \cong b &\mod c \Rightarrow \\ a - b \cong 0 &\mod c \Rightarrow \\ c&|(a-b) \end{aligned}$$

This means that c is a factor of $a - b$. For example, $30 \cong 2 \mod 4$ since $30 - 2 = 28$ and 4 is a factor of 28. When working in mod 5,

$$0 \cong 5 \cong 10 \cong 15 \cong ... \mod 5$$

$$1 \cong 6 \cong 11 \cong 16 \cong ... \mod 5$$

$$2 \cong 7 \cong 12 \cong 17 \cong ... \mod 5$$

Thus, in mod 5, there are only 5 elements: 0, 1, 2, 3, and 4.

Mathematical Focus 2: A Field

A **Field** is a set of elements with every non-zero element having a **Multiplicative Inverse**. The set $\{0, 1, 2, 3, 4\}$ is a field because $2 \cdot 3 \cong 1 \mod 5$ and $4 \cdot 4 \cong 1 \mod 5$. 1 is also its own multiplicative inverse.

One of the ways to look at fractions is a convenient notation which when added to the Integers make them a field. So $\frac{1}{3}$ can be viewed as the multiplicative inverse of 3. The reason we need to introduce this notation with the integers is that 3 does not have a multiplicative in the Integers.

Because Modulo 5 is a **Finite Field**, there is not need to introduce fractions, thus, $\frac{3}{4}$ doesn't even make sense in that field. On the other hand, if we define a fraction 300

Mathematical Focus 3: Multiplicative Inverse

Fractional notation is actually a convenient way of writing multiplicative inverses of elements of a certain set of numbers. A **multiplicative inverse** is defined as an element a^{-1} such that:

$$a^{-1} \cdot a = a \cdot a^{-1} = 1$$

When we are working with rational and real numbers, $\frac{1}{a}$ is essentially the multiplicative inverse of the element a, because:

$$\frac{1}{a} \cdot a = 1 = a \cdot a^{-1}$$

The elements in modulo 5 are $\{0, 1, 2, 3, 4\}$. So $\frac{1}{2} \mod 5$ is an element a such that:

$$a \cdot 2 \cong 1 \mod 5$$

Let's examine the possibilities:

$$\begin{aligned}
1 \cdot 2 &\cong 2 \mod 5 \\
2 \cdot 2 &\cong 4 \mod 5 \\
3 \cdot 2 &\cong 6 \mod 5 \cong 1 \mod 5 \\
4 \cdot 2 &\cong 8 \mod 5 \cong 3 \mod 5 \\
0 \cdot 2 &\cong 0 \mod 5
\end{aligned}$$

So $\frac{1}{2} = 2^{-1} = 3 \mod 5$. Similarly, we find the following unit fractions in mod 5:

$$\frac{1}{3} = 2 \mod 5$$

$$\frac{1}{4} = 4 \mod 5$$

Mathematical Focus 4: Equivalence Classes

$\frac{a}{b}$ can be thought of as the fraction $\frac{1}{b}$, a times. So $\frac{a}{b} = a \cdot \frac{1}{b}$. This is tied into the concept of multiplication as repeated addition. Thus, since $\frac{1}{4} = 4$ mod 5:

$$\frac{3}{4} = 3 \cdot \frac{1}{4} \cong 3 \cdot 4 = 12 \cong 2 \mod 5$$

One of the things which makes fractional notation function is the notion of an **equivalance class**. Two fractions, $\frac{a}{b}$ and $\frac{c}{d}$ are in the same equivalence class if the following is true:

$$\frac{a}{b} = \frac{c}{d}$$
$$\Rightarrow$$
$$ad - cb = 0$$

So if we are to talk about $\frac{3}{4}$, we hope that it's in the same equivalence class as $\dfrac{6}{8}$. This is true though. Suppose we can define a fraction $\dfrac{6}{8} \cong a \mod 5$.

$$\frac{6}{8} \cong a \mod 5$$

$$6 \cong 8a \mod 5$$

$$3 \cong 4a \mod 5$$

$$\frac{3}{4} \cong a \mod 5$$