MAC-CPTM Situations Project

Situation 54(PN6): Modular Arithmetic

Prepared at the
University of Georgia Center for Proficiency in Teaching Mathematics
29 July 2006 – Pawel Nazarewicz

Edited at Pennsylvania State University
Mid-Atlantic Center for Mathematic Teaching and Learning
29 September 2009 -- Glen Blume, Heather Godine, Svetlana Konnova, and Jeanne Shimizu

Prompt

A group of high school Mathematics Club members was examining the concept of modular arithmetic. They were working in mod 5, and as they were becoming familiar with mod 5, a student asked whether it is possible to write fractions in mod 5. For example, what is the meaning of $\frac{3}{4} \bmod 5$?

Commentary

The symbol "$\frac{a}{b}$" such that *a* and *b* are integers and b≠0 can be interpreted in a variety of ways: as a single rational number (commonly called "fraction,") as a ratio of two numbers, or as a quotient of two numbers. However, these interpretations may cause confusion when dealing with operations within integer fields Z_n (where *n* is a positive integer). Thus it is important to move beyond the previously mentioned common interpretations of the symbol "$\frac{a}{b}$" and only regard it as a symbol.

When doing modular arithmetic, it does not make sense to refer to $\frac{a}{b}$ as a fraction, where *b* is not a factor of *a,* because the congruence relation mod *m* (for *m* a positive integer) is defined only for integers. This is discussed in Mathematical Focus 1. However, one can refer to $\frac{a}{b} \bmod m$ as an expression that has meaningful interpretations. If $\frac{a}{b} \bmod m$ is to have meaning, then it must be an element of a finite field, Z_m, as described in Mathematical Focus 2. In Mathematical Focus 3, $\frac{a}{b}$ is interpreted to represent *a* times the multiplicative inverse of *b*. In Mathematical Focus 4, $\frac{p}{q}$ is interpreted as the solution, *x*, to the congruence statement $qx \equiv p \bmod m$, where *p*, *q*, and *m* are integers, *m* is prime, and *q* is not congruent to 0 mod *m*. Mathematical Focus 5 addresses the idea of congruence classes for numbers mod *m* and the conditions necessary for the expressions $\frac{a}{b} \bmod m$ and $\frac{c}{d} \bmod m$ to be in the same congruence class.

Given an expression of the form $\frac{a}{b} \bmod m$, one can ask how to find a value that it can represent in mod *m*. Mathematical Focus 6 presents a type of Greedy Algorithm that can be used, in general, to find such a value.

Mathematical Foci

Mathematical Focus 1

The congruence relation mod m *(for* m *a positive integer) is defined only for integers.*

By definition, if *a, b*, and *m* are integers with *m* > 0, then "*a* is said to be congruent to *b* modulo *m,* if $m \mid (a-b)$" (Strayer, 1994, p. 38). In other words, integer *a* is congruent to integer *b* modulo *m,* if positive integer *m* is a factor of $a-b$.

The statement "*a is congruent to b modulo m"* is written $a \equiv b \bmod m$, where *b is* called the *residue* or the *remainder* and *m* is called the modulus. Commonly used residues for mod *m* are non-negative integers less than *m*. For example, $30 \equiv 2 \bmod 4$ because 4 is a factor of (30–2). (Note: If $(a-b)$ is not integrally divisible by *m*, then it is said that "*a* is not congruent to *b* modulo m.")

Thus, by definition, if $\frac{3}{4}$ is interpreted to represent a number (e.g., a point on the number line halfway between $\frac{1}{2}$ and 1), then $\frac{3}{4} \bmod 5$ does not make sense because $\frac{3}{4}$ is not an integer.

Mathematical Focus 2

Modular arithmetic occurs in a mathematical system of elements, operations on those elements, and properties that hold for those operations with those elements. Z_m, the integers modulo m (for prime m), form a mathematical system that is a finite field.

A *field* is a set, F, of elements together with two operations, addition (denoted as +) and multiplication (denoted as *), that satisfies the field axioms:

Axiom	Addition	Multiplication
Closure	Set F is closed under addition: a and b in F implies $a + b$ is in F.	Set F is closed under multiplication: a and b in F implies $a * b$ is in F.
Associativity	For all a, b, and c in F, $(a+b)+c = a+(b+c)$.	For all a, b, and c in F, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.
Commutativity	For all a, b in F, $a+b=b+a$.	For all a, b in F, $a \cdot b = b \cdot a$.
Existence of identities	There is an element 0 in F such that for all a in F, a + 0 = a.	There is an element 1 in F such that for all a in F, a * 1 = a.
Existence of inverses	For all a in F, there is an element –a in F such that $a + (-a) = 0$.	For all $a \neq 0$ in F, there is an element a^{-1} (or $\frac{1}{a}$) in F such that $a * (a^{-1}) = 1$ or $a * (\frac{1}{a}) = 1$.
Distributivity	For all a, b, and c in F, $a * (b + c) = a * b + a * c$.	

Z_m, the integers modulo m (for m prime), consists of a set of integers {0, 1, 2, ..., (m–1)} together with the operations of integer addition and integer multiplication. Z_m (m prime) forms a mathematical system that is a *finite field*, because Z_m has a finite number of elements and satisfies all the field axioms (see Niven & Zuckerman, 1966, p. 65, for a proof that Z_m is a field iff m is prime.)

Each element of Z_m can be interpreted as a representative of an equivalence class created by the congruence relation $a \equiv b$ modulo m. For example, in Z_5 there are 5 elements, typically denoted by the standard class representatives 0, 1, 2, 3, and 4.

$$[0] = \{\ldots, -10, -5, 0, 5, 10, \ldots\} = \{5n, n \in Z\}$$
$$[1] = \{\ldots, -9, -4, 1, 6, 11, \ldots\} = \{5n + 1, n \in Z\}$$
$$[2] = \{\ldots, -8, -3, 2, 7, 12, \ldots\} = \{5n + 2, n \in Z\}$$
$$[3] = \{\ldots, -7, -2, 3, 8, 13, \ldots\} = \{5n + 3, n \in Z\}$$
$$[4] = \{\ldots, -6, -1, 4, 9, 14, \ldots\} = \{5n + 4, n \in Z\}$$

Because Z_5 is a finite field and thus closed, if ¾ mod 5 has meaning, then it must be some element of one of the equivalence classes for which one of the elements of Z_5 is a representative.

Mathematical Focus 3

A meaning can exist for $\frac{p}{q}$ *mod* m *by considering* $\frac{p}{q}$ *mod* m *to represent the product of* p *and the multiplicative inverse of* q *in mod* m*, where* p *and* q *are integers,* m *is prime, and q is not congruent to* 0 *mod* m.

A multiplicative inverse (if it exists) is an element, a^{-1}, such that $a^{-1} \cdot a = a \cdot a^{-1} = 1$. When working in the rational numbers, the number $\frac{1}{a}$ is the multiplicative inverse of a ($a \neq 0$), because $\frac{1}{a} \cdot a = a \cdot \frac{1}{a} = 1$. When working in a modular system with a prime modulus, each non-zero element in the set will have a multiplicative inverse (see Niven & Zuckerman, 1966, p. 65, for a proof that Z_m is a field iff m is prime).

To answer the question, "What is the meaning of $\frac{3}{4} \bmod 5$?" one can interpret $\frac{3}{4} \bmod 5$ to represent the product of 3 and $\frac{1}{4}$, such that the symbol "$\frac{1}{4}$" is interpreted as the multiplicative inverse of 4 in mod 5. Note that the product of a non-zero number and its multiplicative inverse is one.

For example, to find the multiplicative inverse of 4, consider each of the non-zero congruence classes mod 5,

$$[1] = \{\ldots, -9, -4, 1, 6, 11, \ldots\} = \{5n + 1, n \in Z\}$$
$$[2] = \{\ldots, -8, -3, 2, 7, 12, \ldots\} = \{5n + 2, n \in Z\}$$
$$[3] = \{\ldots, -7, -2, 3, 8, 13, \ldots\} = \{5n + 3, n \in Z\}$$
$$[4] = \{\ldots, -6, -1, 4, 9, 14, \ldots\} = \{5n + 4, n \in Z\},$$

multiply the general expression for a representative of the class by 4 and determine whether or not the resulting product is congruent to 1 mod 5. This is equivalent to asking the question, "Is 5 a factor of the number that is one less than the resulting product?"

For [1] (4)(5n + 1) = 20n +4. Given that 5 is not a factor of (20n + 4) – 1, (4)(5n + 1) is not congruent to 1.

For [2], (4)(5n + 2) = 20n + 8. Given that 5 is not a factor of (20n + 8) – 1, (4)(5n + 1) is not congruent to 1.

For [3], (4)(5n + 3) = 20n + 12. Given that 5 is not a factor of (20n + 12) – 1, (4)(5n + 1) is not congruent to 1.

For [4], (4)(5n + 4) = 20n + 16. Given that 5 IS a factor of (20n + 16) – 1, (4)(5n + 1) IS congruent to 1. Therefore, the multiplicative inverse of 4 is 4.

Given that 3(4)=12 and $12 \equiv 2 \bmod 5$, if one interprets the expression $\frac{3}{4} \bmod 5$ to represent (the product of 3 and the multiplicative inverse of 4) mod 5, then the expression $\frac{3}{4} \bmod 5$ represents 2 mod 5.

Mathematical Focus 4

A meaning can exist for $\frac{p}{q} \bmod m$ *by considering* $\frac{p}{q} \bmod m$ *to represent* x *such that* $px \equiv q \ mod \ m$*, where* p, q, *and* m *are integers,* m *is prime, and* q *is not congruent to* 0 *mod* m.

Based on what it means to be congruent modulo *m*, the congruence classes mod 5 are:

$$[0] = \{\ldots, -10, -5, 0, 5, 10, \ldots\} = \{5n, n \in Z\}$$
$$[1] = \{\ldots, -9, -4, 1, 6, 11, \ldots\} = \{5n + 1, n \in Z\}$$
$$[2] = \{\ldots, -8, -3, 2, 7, 12, \ldots\} = \{5n + 2, n \in Z\}$$
$$[3] = \{\ldots, -7, -2, 3, 8, 13, \ldots\} = \{5n + 3, n \in Z\}$$
$$[4] = \{\ldots, -6, -1, 4, 9, 14, \ldots\} = \{5n + 4, n \in Z\}.$$

To answer the question, "What is the meaning of $\frac{3}{4} \bmod 5$?" one can interpret $\frac{3}{4}$ to represent "x such that $4x \equiv 3 \bmod 5$." Examining the set of values congruent to 3 mod 5 for multiples of 4, without loss of generality, choose the smallest positive multiple of 4, namely 8, and solve the resulting congruence statement for x.

$$\begin{aligned} 4x &\equiv 8 \bmod 5 \\ x &\equiv 2 \bmod 5 \end{aligned}$$

Therefore, if $\frac{3}{4} \bmod 5$ is interpreted to represent x such that $4x \equiv 3 \bmod 5$, then x, and thus $\frac{3}{4} \bmod 5$, represents $2 \bmod 5$.

Mathematical Focus 5

A necessary and sufficient condition for $\frac{p}{q} \bmod m$ *and* $\frac{r}{s} \bmod m$ *to be in the same congruence class is* $ps \equiv (qr) \bmod m$.

For integers *p*, *q*, *r*, *s*, and *m* ($p, s \not\equiv 0 \bmod m$ and *m* prime), $\frac{p}{q} \bmod m$ and $\frac{r}{s} \bmod m$ are in the same congruence class if and only if $ps \equiv (qr) \bmod m$, or $\frac{p}{q} \equiv \frac{r}{s} \bmod m \leftrightarrow ps \equiv (qr) \bmod m$. The proof that follows uses the interpretation that $\frac{x}{y} \bmod m$ represents $(x \cdot \text{multiplicative inverse of } y) \bmod m$ for integers *x, y, m* ($y \not\equiv 0 \bmod m$ and *m* > 0), and the symbol, y^{-1}, will be used to represent the multiplicative inverse of *y*.

<u>Proof</u>
For integers *p, q, r, s*, and *m*, where *p* and *s* are not congruent to $0 \bmod m$ and where *m* is prime:

If $\frac{p}{q} \equiv \frac{r}{s} \bmod m$, then $ps \equiv (qr) \bmod m$.

$$\frac{p}{q} \equiv \frac{r}{s} \bmod m$$

Using the interpretation that $\frac{x}{y} \bmod m$ represents $(x \cdot \text{multiplicative inverse of } y) \bmod m$ for integers *x, y, m* ($y \not\equiv 0 \bmod m$ and *m* > 0),

$$p\left(q^{-1}\right) \equiv \left\{r\left(s^{-1}\right)\right\} \bmod m.$$

Multiplying each side of the congruence by *s*,

$$p\left(q^{-1}\right)s \equiv \left\{r\left(s^{-1}\right)s\right\} \bmod m.$$

Because the product of a number and its multiplicative inverse is 1,

$$p\left(q^{-1}\right)s \equiv r \bmod m.$$

Commuting *s* and the multiplicative inverse of *q*,

$$ps\left(q^{-1}\right) \equiv r \bmod m.$$

Multiplying each side of the congruence by *q,*

$$ps\left(q^{-1}\right)q \equiv (rq) \bmod m.$$

So,

$$ps \equiv (qr) \bmod m.$$

Therefore, if $\frac{p}{q} \equiv \frac{r}{s} \bmod m$, then $ps \equiv (qr) \bmod m$.

If $ps \equiv (qr) \bmod m$, then $\frac{p}{q} \equiv \frac{r}{s} \bmod m$.

$$ps \equiv (qr) \bmod m$$

Multiplying each side of the congruence by the multiplicative inverse of s, s^{-1},

$$p \equiv (qrs^{-1}) \bmod m.$$

Thus,

$$p \equiv \left\{q\left(\tfrac{r}{s}\right)\right\} \bmod m.$$

Multiplying each side of the congruence by the multiplicative inverse of q, q^{-1}, and using the commutative property,

$$pq^{-1} \equiv \left\{qq^{-1}\left(\tfrac{r}{s}\right)\right\} \bmod m.$$

Because the product of a number and its multiplicative inverse is 1,

$$pq^{-1} \equiv \tfrac{r}{s} \bmod m \text{, or } \tfrac{p}{q} \equiv \tfrac{r}{s} \bmod m.$$

Therefore, if $ps \equiv (qr) \bmod m$, then $\frac{p}{q} \equiv \frac{r}{s} \bmod m$.

So, $\frac{p}{q} \bmod m$ and $\frac{r}{s} \bmod m$ are in the same congruence class if and only if $ps \equiv (qr) \bmod m$.

Applying this theorem to $\frac{3}{4} \bmod 5$ leads to several conclusions:

(i) $\frac{3}{4} \bmod 5$ is in the same congruence class as $\frac{p}{q} \bmod 5$ if and only if $3q \equiv 4p \bmod 5$.

(ii) $\frac{3}{4} \bmod 5$ and $\frac{6}{8} \bmod 5$, are in the same congruence class.

The products of (3)(8) and (6)(4) are both congruent to $4 \bmod 5$. This result is not surprising, given that $\frac{3}{4}$ and $\frac{6}{8}$ are equivalent fractions in the real number system.

(iii) $\frac{3}{4} \bmod 5$ and $\frac{3k}{4k} \bmod 5$ ($k \neq 0$), are in the same congruence class.

The products (3)(4k) and (4)(3k) are both congruent to $(12k) \bmod 5$.

(iv) $\frac{3}{4} \bmod 5$ and $\frac{6}{13} \bmod 5$ are in the same congruence class.

The products of (3)(13) and (6)(4) are both congruent to $4 \bmod 5$. This may be counterintuitive because $\frac{3}{4}$ and $\frac{6}{13}$ are not equivalent fractions in the real number system.

(v) $\frac{3}{4} \bmod 5$ and $\frac{3+5k}{4+5k} \bmod 5$ (k an integer) are in the same congruence class.

The products (3)(4 + 5k) and (4)(3 + 5k) are congruent to $12 \bmod 5$ and therefore, $2 \bmod 5$.

(vi) $\frac{3}{4} \bmod 5$ and $\frac{3+5j}{4+5k} \bmod 5$ (j and k integers) are in the same congruence class.
The products $(3)(4 + 5k)$ and $(4)(3 + 5j)$ are both congruent to $12 \bmod 5$, which is congruent to $2 \bmod 5$.

Mathematical Focus 6

The value of $\frac{p}{q} \bmod m$ *(*q *and* m *are relatively prime,* m *prime) can be found using a type of Greedy Algorithm.*

To find a value for $\frac{p}{q}$ mod m, where q and m are relatively prime and m is prime, one can use an algorithm similar to a Greedy Algorithm (Weisstein, 2009)—an algorithm used to recursively construct a set of objects from the smallest possible constituent parts.

Let $q_0 \equiv q \bmod m$ and find $p_0 = \left\lceil \frac{m}{q_0} \right\rceil$, where $f(x) = \lceil x \rceil$ is the ceiling function that gives the least integer greater than or equal to x.

Next, compute $q_1 \equiv (q_0 \cdot p_0) \bmod m$. From $i = 1$, iterate $p_i = \left\lceil \frac{m}{q_i} \right\rceil$ and $q_{i+1} \equiv (q_i \cdot p_i) \bmod m$, until $q_n = 1$. Then $\frac{p}{q} \equiv \left(p \cdot \prod_{i=0}^{n-1} p_i \right) \bmod m$. (This method always works for m prime.)

Applying this method to find $\frac{3}{4} \bmod 5$, $p = 3$, $q = 4$, and $m = 5$.
So, $q_0 \equiv 4 \bmod 5$, and $p_0 = \left\lceil \frac{m}{q_0} \right\rceil = \left\lceil \frac{5}{4} \right\rceil = 2$.
Then, $q_1 \equiv q_0 \cdot p_0 \equiv 4 \cdot 2 \equiv 3 \bmod 5$, and $p_1 = \left\lceil \frac{m}{q_1} \right\rceil = \left\lceil \frac{5}{3} \right\rceil = 2$.
Finally, $q_2 \equiv q_1 \cdot p_1 \equiv 3 \cdot 2 \equiv 1 \bmod 5$, making $n = 2$.

So, $\frac{3}{4} \equiv p \cdot \prod_{i=0}^{2-1} p_i \equiv p \cdot p_0 \cdot p_1 \equiv 3 \cdot 2 \cdot 2 \equiv 2 \bmod 5$.

Therefore, $\frac{3}{4} \equiv 2 \bmod 5$.

Post-Commentary

A meaning for $\frac{3}{4} \bmod 5$ exists because 5 is prime and therefore every nonzero element in Z_5 has a multiplicative inverse. However, for Z_m with m composite, the multiplicative inverse of a nonzero element may not exist.

Suppose one wished to find the value represented by $\frac{3}{4} \bmod 6$. Consider the multiplication table for mod 6:

•	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

The products 1 times 1 and 5 times 5 both equal 1. Therefore, 1 is its own multiplicative inverse, and 5 is its own multiplicative inverse. Also, no other product of two values equals 1. Therefore, multiplicative inverses for 0, 2, 3, and 4 do not exist.

Because (multiplicative inverse of 4) mod 6 does not exist, $\frac{3}{4} \bmod 6$, as defined to be the product {3 and (multiplicative inverse of 4)} mod 6 does not exist.

References

Niven, I., & Zuckerman, H. S. (1966). *An introduction to the theory of numbers*. New York: Wiley.

Strayer, J. K. (1994). *Elementary number theory*. Long Grove, IL: Waveland Press.

Weisstein, E. W. (n.d.). *Congruence*. Retrieved September 14, 2009, from Wolfram MathWorld Web site: http://mathworld.wolfram.com/Congruence.html