

## Times versus Plus

Very often rules obeyed by plus are also rules for times. For example, commutative rules hold for both operations:

$$a + b = b + a$$

and

$$a \times b = b \times a.$$

On the other hand, sometimes you get in big trouble when you replace “+” by “ $\times$ .” This confusion is one of the single most common errors in arithmetic and algebra. The rule for multiplying fractions

$$\frac{a}{b} \times \frac{c}{d} = \frac{a \times c}{b \times d}$$

leads to the **totally wrong** “rule”

$$\frac{a}{b} + \frac{c}{d} = \frac{a + c}{b + d}.$$

It may interest you to know that this “wrong addition” has been well studied by number theorists, but it is **not** the way we add fractions.

Similarly, the derivative rule for sums

$$(f + g)' = f' + g'$$

leads to one of the favorite “freshman” rules of beginning calculus students

$$(f \cdot g)' = f' \cdot g'.$$

This **totally wrong** product rule would imply that

$$\frac{d}{dx}x^2 = \frac{d}{dx}x \cdot \frac{d}{dx}x = 1 \cdot 1 = 1$$

and hence

$$\frac{d}{dx}x^n = 1$$

by induction, thereby making calculus completely useless.

This introduction brings us to the definition of addition and multiplication of sets. If  $A$  and  $B$  are sets, then we define

$$A + B \stackrel{\text{def}}{=} \{x + y : x \in A \text{ and } y \in B\}.$$

We can use this definition to define addition of congruence classes, namely

$$[a]_n + [b]_n \stackrel{\text{def}}{=} \{x + y : x \in [a]_n \text{ and } y \in [b]_n\}.$$

Under this definition  $[a]_n + [b]_n$  turns out to be precisely  $[a + b]_n$ , as you are asked to prove in Question 3 at the end of this handout.

Let’s consider a simple example with  $n = 5$ ,  $a = 2$ , and  $b = 3$ . Since

$$[2]_5 = \{\dots, -13, -8, -3, 2, 7, 12, \dots\}$$

and

$$[3]_5 = \{\dots, -12, -7, -2, 3, 8, 13, \dots\},$$

the sum of these sets is

$$[2]_5 + [3]_5 = \{\dots, -20, -15, -10, -5, 0, 5, 10, 15, 20, \dots\},$$

which is precisely the congruence class  $[0]_5$ , or equivalently,  $[2 + 3]_5$ .

Now what happens if we replace “+” with “ $\times$ ”? We get

$$A \times B \stackrel{\text{def}}{=} \{x \times y : x \in A \text{ and } y \in B\},$$

a completely natural definition. Using this to define multiplication of congruence classes leads to

$$(1) \quad [a]_n \times [b]_n \stackrel{\text{def}}{=} \{x \times y : x \in [a]_n \text{ and } y \in [b]_n\}.$$

Does it follow that

$$(2) \quad [a]_n \times [b]_n = [a \cdot b]_n?$$

Consider the last example with  $n = 5$ ,  $a = 2$ , and  $b = 3$ . Using the definition of set multiplication given in equation (1), the product of

$$[2]_5 = \{\dots, -13, -8, -3, 2, 7, 12, \dots\}$$

and

$$[3]_5 = \{\dots, -12, -7, -2, 3, 8, 13, \dots\},$$

is

$$[2] \times [3]_5 = \{\dots, -24, -14, -9, -4, 6, 16, 21, \dots\}.$$

The set on the right is **not** the congruence class  $[1]_5$ . Numbers are missing. In particular, you cannot write 1 itself as a product of an element  $x \in [2]_5$  and an element  $y \in [3]_5$ . The same thing goes for any *prime* congruent to 1 mod 5, such as 11 or 31.

Let’s be perfectly clear about this point. If we use (1) to define multiplication of sets, then we always have the set inclusion

$$[a]_n \times [b]_m \subseteq [a \times b]_n,$$

because

$$x \equiv a \pmod{n} \text{ and } y \equiv b \pmod{n} \text{ implies } xy \equiv ab \pmod{n}.$$

But it does not follow that  $[a \times b]_n$  is a subset of  $[a]_n \times [b]_m$ .

Now what do we do? The answer is simple. We use equation (2) to define multiplication of congruence classes. And we abandon (1) as a definition. Is this okay? You betcha, as long as we can demonstrate consistency, as discussed in the text. Mathematicians are like politicians, we get to choose our own rules and definitions. Unlike politicians, we have to live with the rules we choose.

**Question 1.** What are some other examples where rules for  $+$  can be carried over to rules for  $\times$ ?

**Question 2.** What are some other examples where rules for  $+$  cannot be carried over to rules for  $\times$ ?

**Question 3.** For addition, it is true that

$$[a + b]_n = \{x + y : x \in [a]_n \text{ and } y \in [b]_n\}.$$

The set inclusion

$$\{x + y : x \in [a]_n \text{ and } y \in [b]_n\} \subseteq [a + b]_n$$

follows immediately from the fact that if  $x \equiv a \pmod{n}$  and  $y \equiv b \pmod{n}$ , then  $x + y \equiv a + b \pmod{n}$ . Going in the other direction requires us to verify that

$$[a + b]_n \subseteq \{x + y : x \in [a]_n \text{ and } y \in [b]_n\}.$$

Prove that given any element  $z$  in  $[a + b]_n$ , you can always find an element  $x$  in  $[a]_n$  and an element  $y$  in  $[b]_n$  such that  $x + y = z$ .