

## Activity on Binary Operations

### 1. Field Guide Ideas

- (a) List examples of binary operations that you use in your teaching.
  - (b) Select a few of these binary operations and analyze them: is the operation commutative? associative?; does the operation have an identity, and if so, which elements have inverses?
  - (c) Give some examples where the associativity of normal addition is useful.
  - (d) Give some examples where the associativity of normal multiplication is useful.
2. Let  $R$  be the set of all functions from  $X$  to  $X$ . For  $f$  and  $g$  in  $R$ , let  $f \circ g$  be the composition of  $f$  and  $g$ , that is,  $f \circ g : X \rightarrow X$  by  $(f \circ g)(x) = f(g(x))$ .
- (a) Is  $\circ$  associative? Why or why not?
  - (b) Is  $\circ$  commutative? Why or why not?
  - (c) Does  $\circ$  have an identity? If so, what is it?
  - (d) If  $X$  is the set of reals, then what conditions on the graph of  $y = f(x)$  guarantee that  $f$  has an inverse? Graphically, how can you find the inverse of such an  $f$ ?
3. Let  $S$  be a set, and  $P(S)$  the set of all subsets of  $S$ . Consider the binary operation of *intersection*. I.e.  $A \cap B = \{x : x \in A \text{ and } x \in B\}$ .
- (a) Is intersection associative?
  - (b) Is intersection commutative?
  - (c) What is the identity for the intersection operation on  $P(S)$ ?
  - (d) Which elements of  $P(S)$  have inverses?
4. Answer the same questions as in 2, but for the union.
5. Investigate adding points on elliptic curves at:  
[http://www.certicom.com/ecc\\_tutorial/ecc\\_javaCurve.html](http://www.certicom.com/ecc_tutorial/ecc_javaCurve.html)
- (a) Try it for various values of  $a$  and  $b$
  - (b) Play with computing  $P \# P$  (which they call  $2P$ ). See if you can predict the answer before you use the program to verify the answer.
6. Let's consider the elliptic curve  $y^2 = x^3 + 1$
- (a) Verify that each of  $(-1, 0)$ ,  $(0, \pm 1)$  and  $(2, \pm 3)$  is on the curve.

- (b) Complete the following table. (Hint: your answer will always be one of these 6 points; so you can sketch a graph of  $y^2 = x^3 + 1$  and then use the geometric method. Symmetry will also help limit the number of things you need to check.)

#	$\mathcal{O}$	$(-1, 0)$	$(0, 1)$	$(0, -1)$	$(2, 3)$	$(2, -3)$
$\mathcal{O}$						
$(-1, 0)$						
$(0, 1)$						
$(0, -1)$						
$(2, 3)$						
$(2, -3)$						

7. Now let's look at the elliptic curve  $y^2 = x^3 - 2$ .
- Verify that  $P = (3, 5)$  is one the curve.
  - Determine  $P\#P$ . (Hint: Calculus shows that the tangent to the curve at  $(x, y)$  is  $\frac{3x^2}{2y}$ .)
  - Determine  $P\#(P\#P)$ .
8. I have a point  $P$  on an elliptic curve, and I know that  $P\#P = \mathcal{O}$ . What does this mean geometrically? (i.e. what does the curve look like at the point  $P$ ?)