A Field is:

1. A collection F of objects
2. Two binary operations x and + closed on F
3. F contains multiplicative identity 1 where (1 x y) = y for all y in F
4. F contains additive identity 0 where (0 + y) = y for all y in F.
5. For each y in F, there exists a z in F such that (y + z) = 0. (Additive inverse)
6. For each y in F, except 0, there exists a z in F such that (y x z) = 0. (Multiplicative inverse)
7. Associative, commutative, distributive laws work as expected

Shorthands:

* is a’s multiplicative inverse
* -a is a’s additive inverse
* a-b is short for a + -b
* a/b is short for a x

Examples:

* R with standard addition and multiplication form a field.
* Q with standard addition and multiplication form a field.
* Z with standard addition and multiplication DOESN’T form a field. ( doesn’t exists for most a.)
* forms a filed with p prime and addition and multiplication mod p. (p must be prime to make sure every element has a multiplicative inverse.)
* THEOREM: If a is prime, then there is a field of size for each n > 0.
* is not convenient for high-speed processing: mod p is expensive and standard data type don’t hold a prime number of values
* Since 2 is prime there is a field of size for all n > 0. This is promising because all data types can hold power-of-two different values.
* Galois Fields (Évariste Galois died age 20 in a duel, 1823)
* The set of all bit sequences of length n forms a field called GF(). We will use GF(256) in this class.
* GF(256) = {00000000, 00000001, 00000010,…,11111111}

Addition:

* Interpret the bits as coefficients of a degree 7 polynomial with variable x.
* Add the two polynomials, to keep coefficients 0 or 1, mod each coefficient by 2.
* Concat the coefficients of the resulting degree 7 polynomial.
* Shortcut: Xor’ing the two bytes produces the same result.

Example:

10001000

Multiplication:

* Interpret the bits as coefficients of a degree 7 polynomial with variable x.
* Multiply the two polynomials, to keep coefficients 0 or 1, mod each coefficient by 2.
* Mod the result by
* Concat the coefficients of the resulting degree 7 polynomial.
* Shortcut: No shortcut. Multiplication is expensive.

Example:

mod

mod