Galois fields

The wikipedia article on finite fields is pretty dense.

`https://en.wikipedia.org/wiki/Finite_field`

Such fields are called Galois fields and often given a name such as $GF(7)$.

> As with any field, a finite field is a set on which the operations of multiplication, addition, subtraction and division are defined and satisfy certain basic rules. The most common examples of finite fields are given by the integers mod p when p is a prime number.

Previously we looked at modular arithmetic. The integers mod some number, say $n = 6$ or $n = 7$, with addition and multiplication defined in the standard way, form a finite group, with additive and multiplicative identities.

However, to be a **field**, for each element, $\{0, 1, 2, 3, 4, 5, 6\}$, there must be a multiplicative inverse — which may be the element itself. If we lay out the multiplication table for arithmetic mod a prime number, then the row for each element contains all of the elements, including 1. There are pairs of elements that when multiplied together give the multiplicative identity, 1. Sometimes, the pair consists of an element plus itself: $6 \times 6 = 1 \pmod 7$.

The number of elements of a finite field is called its order.

> A finite field of order q exists if and only if the order q is a prime power p^k (where p is a prime number and k is a positive integer).

So apparently, not only prime numbers but prime powers p^k can be used to construct fields. If you look back at the table for arithmetic modulo 9, you'll see that rows for integers which are co-prime to 9 have all the elements, but the rows for 3 and 6 do not.

> In a field of order p^k, adding p copies of any element always results in zero; that is, the characteristic of the field is p... The elements of the prime field of order p may be represented by integers in the range $0, ..., p - 1$.

.

So for a finite field of order q $(= 2^k)$, the characteristic of the field is 2.

> ... the polynomial $X^q - X$ has all q elements of the finite field as roots. The non-zero elements of a finite field form a multiplicative group.

So the business about polynomials apparently arises from the fact that we want to construct a Galois field for $2^8 = 256$, which is not prime, but is expressible as a prime power (of 2).

> This group is cyclic, so all non-zero elements can be expressed as powers of a single element called a primitive element of the field. (In general there will be several primitive elements for a given field.)

We will see much more about primitive elements.

Simple Galois field

GF(2)

GF(2) consists of the set {0,1}.

We define **addition**

$$0 + 0 = 0$$

$$0 + 1 = 1$$

$$1 + 0 = 1$$

$$1 + 1 = 0$$

The last one is the addition that would generate a value not in the set if we didn't have a special definition. Addition is the same as logical XOR.

subtraction

$$0 - 0 = 0$$

$$1 - 0 = 1$$

$$0 - 1 = 1$$

$$1 - 1 = 0$$

Note that $add(x, y)$ is exactly the same as $subtract(x, y)$.

From the first table, the arithmetic inverse of 1 is just 1 since $1 \oplus 1 = 0$.

$$1 - 1 = 0 = 1 + 1 = 0$$

Therefore

$$-1 = 1$$

For a similar reason $0 - 1 = 1$.

Another reason is that in moving 0 to -1 we move by one unit.

multiplication

$$0 \times 0 = 0$$

$$0 \times 1 = 0$$

$$1 \times 0 = 0$$

$$1 \times 1 = 1$$

Multiplication is the same as logical AND.