A Deeper Look Into Her Math

What exactly is characteristic p? My first attempt of a definition of characteristic p was the definition of a characteristic ring. If there is at least a positive integer n such that na = 0, for every a that is an element of R, then R is said to have characteristic n. If no such n exists, R is said to have characteristic 0. This is clear, because zero times any number is equal to zero.

A commutative ring with unity is said to be an integral domain if it has no zero divisors. Thus, a product is zero only when one of the factors is 0; that is, a * b = 0 only when a = 0 or b = 0. This definition, sometimes, but not always holds true for characteristic p since a characteristic p ring does not have to be an integral domain. To explain this a little deeper, a nonzero element a in a commutative ring R is called a zero divisor if there is a nonzero element b in R such that (a * b) = 0. For example, in mod 6, (9 * 2) = 0, which will be explained later. In this case, neither a nor b is equal to zero, but the product is equal to zero. An alternate definition of characteristic p is:

For every r in a ring r + r + r _ _ _ + r = 0.

In this definition, p represents the number of times you must add r in order to get back to zero. Smith refers to characteristic p as clock or modular arithmetic. This explains exactly how we know that (9 * 2) = 0 in mod 6. In whatever modular base you are in (my example is in 6) you divide the base into the product of the terms. The remainder will give you the answer of the product mod 6. Since (9 * 2) = 18, and 6 divides into 18 with a remainder of zero, then the answer to the problem, (9 * 2) mod 6 is zero. When using clock arithmetic, you take the modular number, and that is the number of hours on the clock. In our case we have a six-hour clock. On the clock, zero equals six. The only numbers used on the clock are {0,1,2,3,4,5}, and any other number is equal to one of those numbers. These are also called the remainders in mod 6. Another example would be to think of modulo 3. The numbers on the three-hour clock, or the remainders would be {0,1,2}. If one uses characteristic p definition in mod 3, then

0 + 0 + 0 = 0
1 + 1 + 1 = 0, and
2 + 2 + 2 = 0.

In this definition of mod 3, the remainders are added p times in order to get back to zero. If you think of modulo 4, the numbers on the four-hour clock, or the remainders, would be {0,1,2,3}. The idea of characteristic p is the number of times you have to add the remainders to get back to zero. For example,

0 + 0 + 0 + 0 = 0
1 + 1 + 1 + 1 = 0
2 + 2 + 2 + 2 = 0, and
3 + 3 + 3 + 3 = 0.

It is nice that characteristic p enables us to limit the names of numbers. For instance, every number in mod 4 that is added or multiplied would equal one

of those four numbers, {0,1,2,3}. For instance, (a + b) mod 4 would equal the remainder of (a + b)/4. An example would be (2 + 5) mod 4 = 7 mod 4. Therefore, 7/4 = 1, with a remainder of 3. Thus, (2 + 5) mod 4 = 3.
The same is true for multiplication; (a * b) mod 4 would equal the remainder of (a * b)/4. The following is an example; (3 * 4) mod 4 = 12 mod 4. Therefore, 12/4 = 3 with a remainder of 0. Hence, (3 * 4) mod 4 = 0.

On a different note, I want to mention elliptic curves. This is not actually Smith's math, however, it is interesting to see that these curves can translate back and forth from the algebraic perspective to the geometric version. Smith did not use elliptic curves in her math, but it is a representation of how one may go from the algebraic form to the geometric form. Take a look at the curve $y^2 = x^3 - 2$. This curve has only integer solutions that we know of. This equation will work only if x = 3 and y = 5, or x = 3 and y = -5. This is the algebraic form. Now, take a look at the curve, $y^2 = x^3 - 3x - 5$. One can study this for a long time and still not know if there are any integer solutions. However, if you graph this in the real and complex numbers, you will see a graph that looks like a donut. You would never think this equation would make such a neat geometrical curve.