Introduction to Modular Arithmetic

1. Motivation:

   (a) $\mathbf{N} = \{1, 2, 3, \dots\}$

   (b) $\mathbf{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$

   (c) $\mathbf{Q} = \{\frac{a}{b} \,|\, a, b \in \mathbf{Z} \text{ and } b \neq 0\}$

   (d) $\mathbf{R} = \{ \text{ numbers like} \sqrt{2}, \ln 5, \pi, e\}$

   (e) $\mathbf{C} = \{a + ib \,|\, a, b \in \mathbf{R}\}$

2. Binary is the language that computers speak. A computer follows commands by answering simple questions that have answers of "yes" or "no," which is the same as "true" or "false." These responses are interpreted mathematically as 1 for "yes" and "true" and as 1 for "no" and "false." By putting a bunch of these together in a row, like 100110101110110001, you can represent larger numbers and more complicated ideas. In binary, 1 + 1 = 0, 1 + 0 = 1 and 0 + 0 = 0. You can do addition with stings of 0's and 1's this way. In binary, a string represents a number by adding up it's digits via:
   Reading from right-to-left, the number (0 or 1) in the i^{th} position means that you add 2^{i-1}.

   $$11001 = 1 * 2^4 + 1 * 2^3 + 0 * 2^2 + 0 * 2^1 + 1 * 2^0 = 16 + 8 + 1 = 25$$

   Therefore, you can add string as well.

   $$11001 + 10110 = 101111$$

   which is the same as

   $$25 + 22 = 47$$

3. Tertiary is the same, except you have the number 0, 1, 2 and you use 3 instead of 2 in the above algorithm.

   $21021 = 2 * 3^4 + 1 * 3^3 + 0 * 3^2 + 2 * 3^1 + 1 * 3^0 = 2 * 81 + 1 * 27 + 2 * 3 + 1 * 1 = 196$

4. Modulo is a method of simplifying all the integer (and other types of numbers) into a smaller set. Lets see an example to help explain.

$$23 \text{ mod } 5 = \text{Remainder of } 23/5 = 3$$

If you took all of $\mathbf{Z}$ and modulo-ed out by 5, you would get $\{0, 1, 2, 3, 4\}$. This set is symbolized by $\mathbf{Z}_5$. Binary an more complicated version of

5. $\mathbf{Z}_p$. Let p be a prime number. Then the set $\mathbf{Z}_p = \{0, 1, 2, \ldots, p-1\}$. This set can have numbers from within be added together and multiplied together.

$$(5 + 7 + 12 + 3) \text{ mod } 13 = 27 \text{ mod } 13 = \text{Remainder of } 27/13 = 1$$
$$(5 * 7 * 12 * 3) \text{ mod } 13 = 1260 \text{ mod } 13 = \text{Remainder of } 1260/13 = 12$$

6. $\mathbf{Z}_n$. If the number of modulo is not a prime, only addition can be used. Try this out for yourself.

7. Number Bracelets are series of numbers that close back onto themselves because of modular arithmetic. Choose any integer, prime or not, and then choose two numbers from the set. Add those two number via modular arithmetic to get a third. Then add the second and third numbers to get a fourth. Repeat this process until you get back to the original two numbers.
Example in $\mathbf{Z}_5$:
Start with 3 and 1 and get the series

$$\{3, 1, 4, 0, 4, 4, 3, 2, 0, 2, 2, 4, 1, 0, 1, 1, 2, 3, 0, 3, 3, 1, \ldots\}$$

see it repeats and so you have a bracelet.

Homework: (a) Make a list of 10 prime numbers (1 is not a prime).

(b) Determine the set of numbers that are in $\mathbf{Z}_2, \mathbf{Z}_5, \mathbf{Z}_{10}, \mathbf{Z}_7$.

(c) Make 4 bracelets with 4 different modular numbers (i.e. choose 4 different n for $\mathbf{Z}_n$ and choose a set a "starters" for each n and make a bracelet).

(d) Solve the following:

(24+2345) mod 7

(23*123) mod 5