Modular Arithmetic

Modular arithmetic allows us to "wrap around" numbers on a given interval. We use modular arithmetic daily without even thinking about it. When we tell time, we use hours on the interval 1-12. And when the clock gets to 12, we don't wonder what is going to happen next, we know that the hour "wraps around" to 1 and starts over again. This is modular arithmetic.

The formal definition is as follows:
We are given an integer m>1, called the **modulus**. Then we say that two integers a and b are **congruent** to one another **modulo m** and we write $a \equiv b \pmod{m}$ to mean that the difference a-b is an integral multiple of m.

$46 \equiv 17 \pmod{29}$ because $46 - 17 = 1 \cdot 29$

$84 \equiv 26 \pmod{29}$ because $84 - 26 = 2 \cdot 29$

One other definition that you should know:
Let m be an integer with m>1. For an arbitrary integer a, the **residue of a modulo m** is the unique integer r among 0,1,...,m-1 to which a is congruent modulo m.

In our previous examples, 17 is the residue of 46 modulo 29, and 26 is the residue of 84 modulo 29. We can also do this with negative numbers. For example, 5 is the residue of -7 modulo 6.

There are a few important properties of modular arithmetic that will be helpful.

1. Equivalence modulo m preserves sums.
2. Equivalence modulo m preserves products.
3. Because of the two above properties, when we do arithmetic modulo m, we can replace the sum or product of two numbers by its residue modulo m without changing the result.

This means that when we are doing our matrix operations, we can freely take residues modulo m and do arithmetic modulo m in place of standard matrix multiplication and addition, without changing our result. This will be very useful later on! [1]

In the table below are all of the multiplicative inverses modulo 29 of the nonzero elements of our alphabet. We will use these values later on when calculating the inverse key.

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
1	15	10	22	6	5	25	11	13	3	8	17	9	27	2	20	12	21	26	16	18	4	24	23	7	19	14	28

You have now completed the brief modular arithmetic tutorial! Click here to return to the explanation of Hill ciphers.

Last modified *Tue 1 December 2009*.