MATH 110 Tutorial 10

Modular arithmetic can be thought of as doing calculations on **remainders** upon division by a given number.

We compute the (multiplicative) *inverse* of a modulo p by computing the extended Euclidean algorithm on a, p.

We can use the information of an inverse to solve a linear equation. Consider the equation $ax = b \mod p$. If a is non-zero modulo p, we can compute the inverse of a, and multiply both sides of the equation by a^{-1}:

$$a^{-1}(ax) = (a^{-1}a)x = x = a^{-1}b \mod p.$$

There is nothing special about our approach to a single linear equation; this works in general for a set of linear equations. Matrix calculations can be carried out modulo p.

Practice Problems.

1. What is $1 + 2 + 3 + 4 + 5$ modulo 2,3,5 ?
   What is $2 \cdot 4 + 4 \cdot 7 + 5 \cdot 3$ modulo $2, 3, 19$?

2. Compute the inverses of 3 mod 11, 8 mod 13, and 4 mod 7. Use your answers to solve the equations $3x + 2 = 8$ mod 11, $8x - 3 = 6$ mod 13, $4x = 0$ mod 7.

3. Determine the complete solution set for the following systems of equations.

$$(a) \quad \begin{array}{rcl} 4x + 2y & = & 2 \\ 5x - 3y & = & 1 \quad \text{mod } 7 \end{array} \qquad (b) \quad \begin{array}{rrcl} x & + 2y & = & 0 \\ 2x & - y & = & 0 \quad \text{mod } 3 \end{array}$$

$$(c) \quad \begin{array}{rrrcl} 3x & + 4y & + 2z & = & 1 \\ 5x & - 2y & + z & = & 1 \\ x & + 5y & + 6z & = & 1 \quad \text{mod } 7 \end{array}$$

4. *Challenge.* For what values of a does $ax = 1$ have a solution modulo 4 ?