Math 406 Section 4.1: Introduction to Congruences

1. **Introduction:** When attempting to prove things about integers it can often be the case that we can make the question easier than it is at first glance. For example suppose we wished to find integers x, y such that $2x^2 + 8y = 11$. We might make the observation that the left side is even but the right side is odd and so no solution exists. What we have done here is changed the problem (check all numbers) to a simpler problem (check evens and odds). The language of congruences is a more sophisticated version of this.

2. **Definition and Equivalencies:**

   (a) **Definition:** Let $m \in \mathbb{Z}^+$ and $a, b \in \mathbb{Z}$. We say that a and b are congruent mod(ulo) m if $m \mid (b-a)$. We write $a = b \bmod m$ or $a \equiv b \bmod m$ or $a \equiv_m b$ although the latter can be confusing in later contexts. Sometimes we also write $a \bmod m = b$ although this generally happens in computer science when we think of mod as a function. The value m is the *modulus*.

   Example: We have $56 \equiv 23 \bmod 11$ because $11 \mid (56-23)$ and we have $56 \not\equiv 23 \bmod 12$ because $12 \nmid (56-23)$.

   (b) **Theorem/Proof:** Given that $m \mid (a-b)$ iff there is some c with $mc = a - b$ iff $a = b + mc$ we can say that $a \equiv b \bmod m$ iff there is some c with $a = b + mc$. $\mathcal{QED}$

3. **Properties:**

   (a) **Theorem (Congruence Properties):** Congrence acts like equality in the following sense:

      i. $a \equiv a \bmod m$

      ii. $a \equiv b \bmod m$ iff $b \equiv a \bmod m$

      iii. If $a \equiv b \bmod m$ and $b \equiv c \bmod m$ then $a \equiv c \bmod m$.

      iv. If $a \equiv b \bmod m$ and $c \equiv d \bmod m$ then $a \pm c \equiv b \pm d \bmod m$.

      v. If $a \equiv b \bmod m$ and $c \equiv d \bmod m$ then $ac \equiv bd \bmod m$.

      vi. If $a \equiv b \bmod m$ then $a^k \equiv b^k \bmod m$.

   (b) **Theorem (Division Issues):** You might notice that division is lacking here. There are two reasons for this.

   First, when we divide integers we may not get integers.
   Example: We know $2 \equiv 8 \bmod 6$ but it makes no sense to write $2/3 \equiv 8/3 \bmod 6$.

   Second, even when we do get integers the resulting statement may be false.
   Example: We know $2 \equiv 8 \bmod 6$ but we can't divide by 2 to get $1 \equiv 4 \bmod 6$ as this is not true.

   Of course sometimes it is true:
   Example: We know that $2 \equiv 12 \bmod 5$ and we can divide by 2 to get $1 \equiv 6 \bmod 5$.

   What is going on here is encapsulated in the following theorem:

   Theorem: If $ac \equiv bc \bmod m$ then $a \equiv b \bmod m/\gcd(m, c)$. In other words we may cancel an integer from both sides provide we divide the modulus by the gcd of the modulus and the integer we're canceling.

   Proof: Suppose $ac \equiv bc \bmod m$ so that there is some k with $km = ac - bc$ and so we have:

$$k\left(\frac{m}{\gcd(m,c)}\right) = \left(\frac{c}{\gcd(m,c)}\right)(a-b)$$

   From here we get:

$$\frac{m}{\gcd(m,c)} \Bigg| \left(\frac{c}{\gcd(m,c)}\right)(a-b)$$

Now then, by a previous theorem we know that:

$$\gcd\left(\frac{m}{\gcd(m,c)}, \frac{c}{\gcd(m,c)}\right) = 1$$

and so again by a previous theorem we know that:

$$\frac{m}{\gcd(m,c)}\bigg|(a-b)$$

From here we get:

$$a \equiv b \bmod m/gcd(m,c)$$

$\mathcal{QED}$

Example: If we know that $4x \equiv 8y \bmod 50$ then we can conclude that $x \equiv 2y \bmod 50/\gcd(50,4)$ and so $x \equiv 2y \bmod 25$.

4. **Residue Classes:**

(a) **Introduction:** To get started consider the modulus $m = 5$. Notice that under congruence mod 5 all of the integers group into collections which are congruent to one another mod 5:

$$\begin{gathered}
... \equiv -15 \equiv -10 \equiv -5 \equiv 0 \equiv 5 \equiv 10 \equiv 15 \equiv ... \bmod 5 \\
... \equiv -14 \equiv -9 \equiv -4 \equiv 1 \equiv 6 \equiv 11 \equiv 16 \equiv ... \bmod 5 \\
... \equiv -13 \equiv -8 \equiv -3 \equiv 2 \equiv 7 \equiv 12 \equiv 17 \equiv ... \bmod 5 \\
... \equiv -12 \equiv -7 \equiv -2 \equiv 3 \equiv 8 \equiv 13 \equiv 18 \equiv ... \bmod 5 \\
... \equiv -11 \equiv -6 \equiv -1 \equiv 4 \equiv 9 \equiv 14 \equiv 19 \equiv ... \bmod 5
\end{gathered}$$

Every integer is in one of these lines. It follows that we can divide all of $\mathbb{Z}$ into *congruence classes mod 5.* In the above example there are five congruence classes:

$$\begin{gathered}
\{..., -15, -10, -5, 0, 5, 10, 15, ...\} \\
\{..., -14, -9, -4, 1, 6, 11, 16, ...\} \\
\{..., -13, -8, -3, 2, 7, 12, 17, ...\} \\
\{..., -12, -7, -2, 3, 8, 13, 18, ...\} \\
\{..., -11, -6, -1, 4, 9, 14, 19, ...\}
\end{gathered}$$

Note a couple of things:

- Each of these has a particularly nice entry, the smallest nonnegative one. We might take a representative from each class and get the set $\{0, 1, 2, 3, 4\}$.
- There are other ways to pick a representative from each class, for example $\{0, 2, 4, 6, 8\}$. These differ in that they are all even, which may be useful.
- Another example might be $\{0, 2, 4, 8, 16\}$ which are all, except for 0, powers of 2. This may be useful if we are working with powers of 2.

(b) **Definition:** Given a modulus m the integers $\mathbb{Z}$ separate into m distinct *congruence classes mod m.*

(c) **Definition:** Given a modulus m a *complete set of residues mod m* is a set of m integers with the property that any integer is equivalent to exactly one integer in the set.

(d) **Theorem:** If S is a set of m integers no two of which are congruent mod m then S forms a complete set of residues mod m.

Proof: If $a \in \mathbb{Z}$ were not congruent to anything in S then dividing a by m yields a remainder which does not appear when dividing anything in S by m. This means that in S if we divide everything by m there is a remainder we miss, meaning that there are only $m-1$ remainders, but there are m integers, meaning two have the same remainder as one another when divided by m, which contradicts the fact that no two are congruent mod m.

(e) **Definition:** Given a modulus m the set $\{0, 1, 2, ..., m-1\}$ is the *set of least nonnegative residues mod m.*

(f) **Theorem:** Given a modulus m. Suppose $\{r_1, ..., r_m\}$ is a complete set of residues and suppose $a, b \in \mathbb{Z}$ such that $\gcd(a, m) = 1$, then $\{ar_1 + b, ar_2 + b, ..., ar_m + b\}$ is also a complete set of residues.

Proof: No two of these are congruent mod m because if $ar_i + b \equiv ar_j + b \bmod m$ then $ar_i \equiv ar_j \bmod m$ and we may cancel the a because $\gcd(a, m) = 1$ to get $r_i \equiv r_j \bmod m$, a contradiction. Since no two are congruent mod m and there are m of them they form a complete set of residues.

5. **Fast Exponentiation:** It can often be important to calculate very high powers modulo some m, which means to calculate the least nonnegative residue mod m. For example we know that $2^{503} \equiv a \bmod 5$ for $a = 0, 1, 2, 3, 4$ but which?

There are a couple of way to approach this:

(a) Look for patterns. We will prove some essential number theory congruences later which will formalize this but consider for example that in the example above: $2^1 \equiv 2 \bmod 5$, $2^2 \equiv 4 \bmod 5$, $2^3 \equiv 3 \bmod 5$, $2^4 \equiv 1 \bmod 5$. Using this last one we can see that since $503 = 4(125) + 3$ we have:

$$2^{503} = (2^4)^{125} 2^3 \equiv 1^{125} 3 = 3 \bmod 5$$

(b) Be systematic. For something like $3^{562} \bmod 847$ we can repeatedly square 3 as follows:

$$\begin{aligned}
3^1 &\equiv 3 \bmod 847 \\
3^2 &\equiv 9 \bmod 847 \\
3^4 &\equiv 81 \bmod 847 \\
3^8 &\equiv 81^2 \equiv 632 \bmod 847 \\
3^{16} &\equiv 632^2 \equiv 487 \bmod 847 \\
3^{32} &\equiv 487^2 \equiv 9 \bmod 847 \\
3^{64} &\equiv 81 \bmod 847 \\
3^{128} &\equiv 81^2 \equiv 632 \bmod 847 \\
3^{256} &\equiv 632^2 \equiv 487 \bmod 847 \\
3^{512} &\equiv 487^2 \equiv 9 \bmod 847
\end{aligned}$$

Then note that by decontructing 562 into binary we have $562 = 512 + 32 + 16 + 2$ and so:

$$3^{562} \equiv 3^{512} 3^{32} 3^{16} 3^2 \equiv (9)(9)(487)(9) \equiv 130 \bmod 847$$

This isn't trivial, it takes work to do this final calculation, but the work required for entire problem is in pieces and is more manageable than actually calculating 3^{562} which has over $562 \log(3) \approx 268.14$ digits.