1 The Basics of Modular Arithmetic

1.1 Introduction to Congruences

Suppose you wished to find $x, y \in \mathbb{Z}$ satisfying $2x^2 - 8y = 11$. There is no solution because no matter what, $2x^2 - 8y$ is even and 11 is odd. What if even/odd does not work... what else might? $\underbrace{3x^2 - 15y}_{3|\text{this}} = \underbrace{8}_{3\nmid\text{this}}$ If even/odd or divided by 3 works, there is no guarantee that it works $\underbrace{3x^2 - 15y = 9}_{\text{might work}}$. The idea of modular arithmetic formalizes all of this.

Definition. For $a, b, m \in \mathbb{Z}$ with $m \geq 2$ we write $a \equiv b \bmod m$ which is read as "a and b are congruent modulo m." to mean that $m \mid (a - b)$. A few notes on this,

- Equivalent to saying $m \mid (b - a)$.
- Equivalent to saying $\exists c \in \mathbb{Z}$ such that $mc = a - b$ or $\exists x \in \mathbb{Z}$ such that $mc = b - a$ (definition of divisibility).
- Equivalent to saying that if we divide a and b by m, the remainders are the same.

Ex. $8 \equiv 18 \bmod 5$ in fact $8 \equiv 18 \equiv 3 \equiv -2 \equiv 23 \equiv \cdots \bmod 5$. Here with remainder 3. Also note $5 \mid (18 - 8)$ and $5 \mid (8 - 18)$.

Even/odd is the same as $m = 2$.

CS Note. In computer science we often define $\text{mod}(a, m) =$ remainder when $a/m = a\%m$. It is not uncommon to see $a = b \bmod m$ or $a \equiv_m b$ (strongly discouraged).

Moving forward, please use $a \equiv b \bmod m$.

Theorem. Congruence acts like an equals sign in the following sense:

(i) $a \equiv a \bmod m$ (Reflexive).

(ii) if $a \equiv b \bmod m$ then $b \equiv a \bmod m$ (Symmetric).

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

Proof. $a \equiv b \bmod m \implies \exists x$ such that $a - b = mx$, $b \equiv c \bmod m \implies \exists y$ such that $b - c = my$. Then $a - c = (a - b) + (b - c) = mx + my = m(x + y)$ so $m \mid (a - c)$ so $a \equiv c \bmod m$. $\square$

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

i.e. If we know $x \equiv y \bmod 5$ we can conclude $x + 7 \equiv y + 7 \bmod 5$ and also $x + 7 \equiv y + 12 \bmod 5$.

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

i.e. If we know $x \equiv y \bmod 5$ then we can conclude $17x \equiv 17y \bmod 5$ but we can also conclude $17x \equiv 12y \bmod 5$

(vi) If $a \equiv b \bmod m$ and $k \in \mathbb{Z}, k \geq 1$ then $a^k \equiv b^k \bmod m$. (Note: we can *not* use different powers!)

Division Issues. First everything must be an integer, so does $2 \equiv 8 \bmod 6 \implies \frac{2}{3} \equiv \frac{8}{3} \bmod 6$ this is garbage because $\frac{2}{3}, \frac{8}{3} \notin \mathbb{Z}$. However, is $2 \equiv 8 \bmod 6 \implies \frac{2}{2} \equiv \frac{8}{2} \bmod 6$ true? No! because $1 \equiv 4 \bmod 6$ is not true. The point is even if division makes both sides integers there is no guarantee that the congruence is preserved!

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

Proof. Suppose $ac \equiv bc \bmod m$, $\exists k \in \mathbb{Z}$ with $mk = ac - bc$. So $mk = c(b - a)$,

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

Note that from a previous theorem we know that:

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

Then the above statement says that $\frac{m}{\gcd(c,m)} \Big| \frac{c}{\gcd(c,m)} (a - b)$ which implies $\frac{m}{\gcd(\mathrm{c,m})} \Big| a - b$. Therefore, $a \equiv b \bmod \frac{m}{\gcd(c,m)}$. $\square$

1.2 Homework