1 Congruence mod d

Recall the following from the *Quotient Remainder handout*:

Theorem 1.1 (Quotient Remainder Theorem)**.** *Given $n \in \mathbb{Z}$ and $d \in \mathbb{Z}^+$, there are* unique *numbers q and r such that*

$$n = dq + r, \quad \textit{where } 0 \leq r < d \tag{1}$$

Here we call q the *quotient* when n is divided by d, and r is the *remainder* when n is divided by d.

We can define a *relation* $\mod d : \mathbb{Z} \to \mathbb{Z}$ as follows:

$$n \mod d = r \iff d \mid n - r \tag{2}$$

Fact: (1) $n \mod d = r \iff r \mod d = n$.

To see this, notice that $n \mod d = r \iff d \mid n - r \iff n - r = dq \iff r - n = d(-q) \iff d \mid r - n \iff r \mod d = n$.

1.1 Notation

The following are equivalent notations for the $\mod d$ relation:

(i) $n = dq + r$

(ii) $n \mod d \equiv r$

(iii) $\mod_d(n) = r$

(iv) $n \equiv_d r$

(v) $n \equiv r \mod d$

2 $\mod d$ is an equivalence relation

Recall from the *Equivalence Relations handout* the following:

Definition 2.1 (Equivalence Relation)**.** *A relation R on a set A* all *is equivalence relation if the relation has* all *of the following properties:*

(1) ***Reflexive:*** *For every $a \in A, aRa$,*

(2) ***Symmetric:*** *For every $a, b \in A$ if aRb then bRa,*

(3) ***Transitive:*** *For every $a, b, c \in A$ if aRb and bRc then aRc.*

Fact (2): $\mod d$ is an equivalence relation.

To see this, notice the following:

1. For any $n \in \mathbb{Z}$, $n \equiv n \mod d$ since $d \mid 0$ and $n - n = 0$,
2. by *Fact (1)*, if $n \equiv r \mod d$ then $r \equiv n \mod d$,
3. if $n \equiv r \mod d$ and $r \equiv s \mod d$, then $n \equiv s \mod d$,
   since $n = dq + r$, $r = dp + s$ and $n = dq + dp + s = d(q + p) + s$.

2.1 Equivalence Classes $\mod d$

Recall again from the *Equivalence Relations handout*:

Definition 2.2. *Given an* equivalence relation R *on a set* A*, for each* $a \in A$ *we define the equivalence class of* a*, denoted* $[a]$ *as follows:*

$$[a] = \{x \in A \mid xRa\}. \tag{3}$$

Fact (3): For $n = dq + r$, $[r]$ is an equivalence class. This follows from Definitions 2.1 and 2.2

Fact (4): $[r_1] = [r_2] \iff r_1 \equiv_d r_2$. To see this, notice the following for $n = dq + r_1$:

(i) If $[r_1] = [r_2]$ then for any $n \in [r_1] = [r_2]$ we have $d \mid n - r_1$ and $d \mid n - r_2$.
Then clearly $d \mid (n - r_2) - (n - r_1)$.
That is, $d \mid r_1 - r_2 \iff r_1 \equiv r_2$,

(ii) if $r_1 \equiv_d r_2$, then $r_1 = dq + r_2$. That is, $n = dk + r_1 = dk + dq + r_2$. Hence $[r_1] = [r_2]$.