Homework 9

Walker Bagley

April 20, 2022

1. $\sim_n := \{(x, y) \in \mathbb{Z} \times \mathbb{Z} | x \equiv y(mod\ n)\}$ is an equivalence relation for $\mathbb{N}_+$

   Proof.

$$\text{Reflexive: let } a \in \mathbb{Z}$$
$$\text{By def, } a \equiv a(mod\ n) \Leftrightarrow n|a - a \Leftrightarrow n|0$$
$$n * 0 = 0 \text{ and } n \in \mathbb{Z}$$
$$(\forall n \in \mathbb{N}_+)(a \equiv a(mod\ n))$$
$$\text{So, } (a, a) \in \sim_n$$

$$\text{Symmetric: let } a, b \in \mathbb{Z} \text{ and assume } (a, b) \in \sim_n$$
$$\text{Then by def, } a \equiv b(mod\ n) \Leftrightarrow n|a - b \Leftrightarrow (\exists k \in \mathbb{Z})((a - b) * k = n)$$
$$\text{If } (b, a) \in \sim_n, \text{ then } n|b - a$$
$$\text{We know that } (a - b) * k = n, \text{ so } (-1) * (a - b) * (-1) * k = n$$
$$\Leftrightarrow (b - a) * (-1) * k = n$$
$$\Leftrightarrow (b - a) * (-k) = n$$
$$\text{Since } -1 \in \mathbb{Z}, (-1) * k = -k \in \mathbb{Z}$$
$$\text{Therefore, } (b, a) \in \sim_n$$

$$\text{Transitive: let } a, b, c \in \mathbb{Z}$$
$$\text{Assume } (a, b) \in \sim_n \wedge (b, c) \in \sim_n$$
$$\text{Then by def, } a \equiv b(mod\ n) \wedge b \equiv c(mod\ n)$$
$$\text{As we proved in class, } a \equiv b(mod\ n) \wedge c \equiv d(mod\ n) \to a + c \equiv b + d(mod\ n)$$
$$\text{Applying this theorem to the above, } a + b \equiv b + c(mod\ n)$$
$$\text{Further, we know that } \sim_n \text{ is reflexive, so } (-b, -b) \in \sim_n \Leftrightarrow -b \equiv -b(mod\ n)$$
$$\text{Applying this theorem again yields } a + b - b \equiv b + c - b(mod\ n) \Leftrightarrow a \equiv c(mod\ n)$$
$$\text{Then, } (a, c) \in \sim_n$$

$$\text{So, } \sim_n \text{ is an equivalence relation}$$

□

2. $Z \subseteq (\mathbb{N} \times \mathbb{N})^2$ s.t. $((a, b), (c, d)) \in Z :\Leftrightarrow a + d = c + b$ is an equivalence relation

   Proof.

$$\text{Reflexive: let } a, b \in \mathbb{N}$$
$$\text{By definition, } a + b = a + b$$
$$\text{Therefore, } ((a, b), (a, b)) \in Z$$

$$\text{Symmetric: let } a, b, c, d \in \mathbb{N} \text{ s.t. } ((a, b), (c, d)) \in Z$$
$$\text{Then by def, } a + d = c + b$$
$$\text{Consider } ((c, d), (a, b)), \text{ then } c + b = a + d$$
$$\text{We know this is true, so } ((c, d), (a, b)) \in Z$$

$$\text{Transitive: let } a, b, c, d, e, f \in \mathbb{N} \text{ s.t. } ((a, b), (c, d)) \in Z \wedge ((c, d), (e, f)) \in Z$$
$$\text{Then by def, } a + d = b + c \text{ and } c + f = e + d$$
$$\text{Adding both equations together yields } a + d + c + f = b + c + e + d$$
$$\text{Cancelling variables, we are left with } a + f = e + b$$
$$\text{Then by def, } ((a, b), (e, f)) \in Z$$

$$\text{So, } Z \text{ is an equivalence relation}$$

□

3. $Q \subseteq (\mathbb{Z} \times \mathbb{Z}_+)^2$ s.t. $((a, b), (c, d)) \in Q :\Leftrightarrow ad = bc$ is an equivalence relation

Proof.

$$\text{Reflexive: let } a, b \in \mathbb{Z}$$
$$\text{By definition, } ab = ab$$
$$\text{Therefore, } ((a, b), (a, b)) \in Z$$

$$\text{Symmetric: let } a, b, c, d \in \mathbb{Z} \text{ s.t. } ((a, b), (c, d)) \in Q$$
$$\text{Then by def, } ad = cb$$
$$\text{Consider } ((c, d), (a, b)), \text{ then } cb = ad$$
$$\text{We know this is true, so } ((c, d), (a, b)) \in Q$$

$$\text{Transitive: let } a, c, e \in \mathbb{Z} \text{ and } b, d, f \in \mathbb{Z}_+ \text{ s.t. } ((a, b), (c, d)) \in Q \wedge ((c, d), (e, f)) \in Q$$
$$\text{Then by def, } ad = bc \text{ and } cf = ed$$
$$\text{Then, } c = \frac{ed}{f} \text{ and } ad = b * \frac{ed}{f}$$
$$\Leftrightarrow adf = bed$$
$$d \text{ cancels out, leaving } af = be$$
$$\text{Then by def, } ((a, b), (e, f)) \in Q$$

$$\text{So, } Q \text{ is an equivalence relation}$$

□

4. RSA encryption: $M := 435$

Proof.

$$\text{Let } x = 59 \text{ and } y = 67$$
$$\textbf{Public modulus: } n = x * y = 3953$$

$$\varphi(n) = (x - 1)(y - 1) = 58 * 66 = 3828$$
$$\text{Choose } e = 17, \text{ because } e \text{ is prime, it is coprime with } x, y \text{ and } 17 < \varphi(n)$$
$$\textbf{Public key: } 17$$

$$\text{Need to find } d \text{ s.t. } ed \equiv 1 (mod\ n) \wedge gcd(d, \varphi(n)) = 1$$
$$\text{Let private modulus } d = 2477$$
$$\text{Using the Euclidean division algorithm, } 3828 = 1 * 2477 + 1351$$
$$2477 = 1 * 1351 + 1126$$
$$1351 = 1 * 1126 + 225$$
$$1126 = 5 * 225 + 1$$
$$gcd(2477, 3828) = 1$$
$$\textbf{Private key: } 2477$$

$$C = M^e (mod\ n) = 435^{17} (mod\ 3953) = 1819$$
$$\textbf{Cipher: } 1819$$

$$\text{Message } M = C^d (mod\ n) = 1819^{2477} (mod\ 3953) = 435$$

□