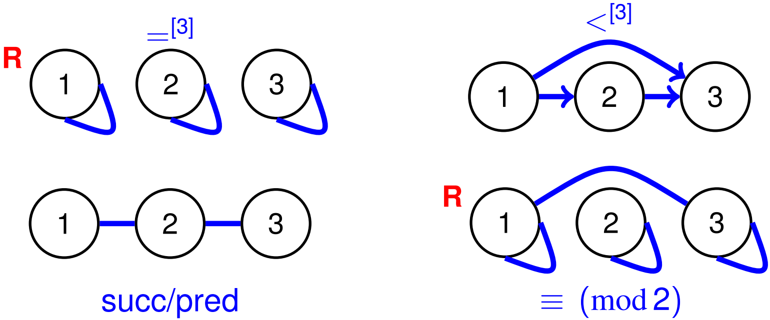
CS250: Discrete Math for Computer Science

L26: Equivalence Relations

Equivalence Relations

Reflexive $\equiv \forall x\, E(x,x)$

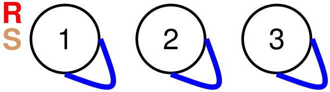


Equivalence Relations

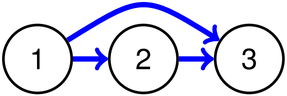
$$\textbf{Reflexive} \equiv \forall x\, E(x,x)$$

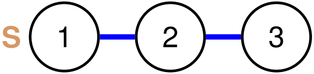
$$\textbf{Symmetric} \equiv \forall xy\, (E(x,y) \rightarrow E(y,x))$$

$=^{[3]}$

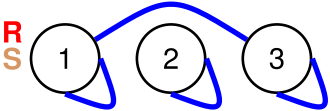


$<^{[3]}$





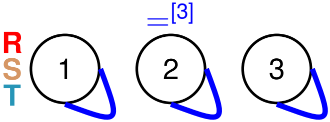
succ/pred

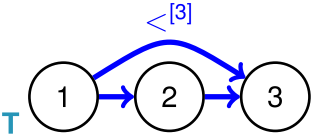


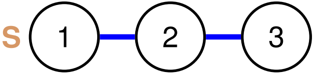
$\equiv \pmod 2$

Equivalence Relations

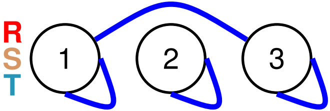
$$\textbf{Reflexive} \equiv \forall x\, E(x,x)$$
$$\textbf{Symmetric} \equiv \forall xy\, (E(x,y) \rightarrow E(y,x))$$
$$\textbf{Transitive} \equiv \forall xyz\, (E(x,y) \wedge E(y,z) \rightarrow E(x,z))$$







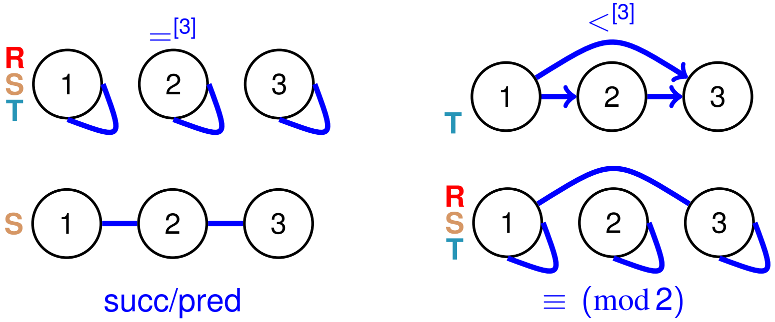
succ/pred



$\equiv \pmod 2$

Equivalence Relations

$$\begin{aligned}
\textbf{Reflexive} &\equiv \forall x\, E(x,x) \\
\textbf{Symmetric} &\equiv \forall xy\, (E(x,y) \rightarrow E(y,x)) \\
\textbf{Transitive} &\equiv \forall xyz\, (E(x,y) \wedge E(y,z) \rightarrow E(x,z))
\end{aligned}$$



Def. An **equivalence relation** is a relation that is **reflexive**, **symmetric** and **transitive**.

Equivalence Relations on 3-Element Sets

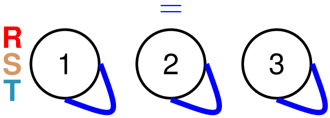
$$\begin{aligned}
\textbf{Reflexive} &\equiv \forall x\, E(x,x) \\
\textbf{Symmetric} &\equiv \forall xy\,(E(x,y) \rightarrow E(y,x)) \\
\textbf{Transitive} &\equiv \forall xyz\,(E(x,y) \wedge E(y,z) \;\rightarrow\; E(x,z))
\end{aligned}$$

Equivalence Relations on 3-Element Sets

$$\textbf{Reflexive} \equiv \forall x\, E(x,x)$$

$$\textbf{Symmetric} \equiv \forall xy\, (E(x,y) \rightarrow E(y,x))$$

$$\textbf{Transitive} \equiv \forall xyz\, (E(x,y) \wedge E(y,z) \rightarrow E(x,z))$$

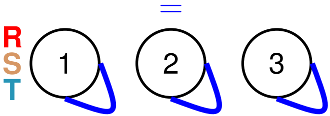


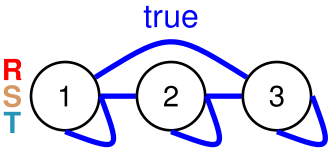
Equivalence Relations on 3-Element Sets

Reflexive $\equiv \forall x\, E(x,x)$

Symmetric $\equiv \forall xy\, (E(x,y) \rightarrow E(y,x))$

Transitive $\equiv \forall xyz\, (E(x,y) \wedge E(y,z) \rightarrow E(x,z))$



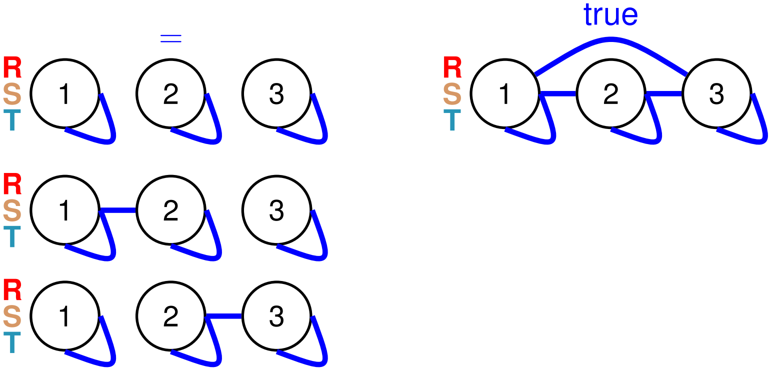


Equivalence Relations on 3-Element Sets

$$\textbf{Reflexive} \equiv \forall x\, E(x,x)$$

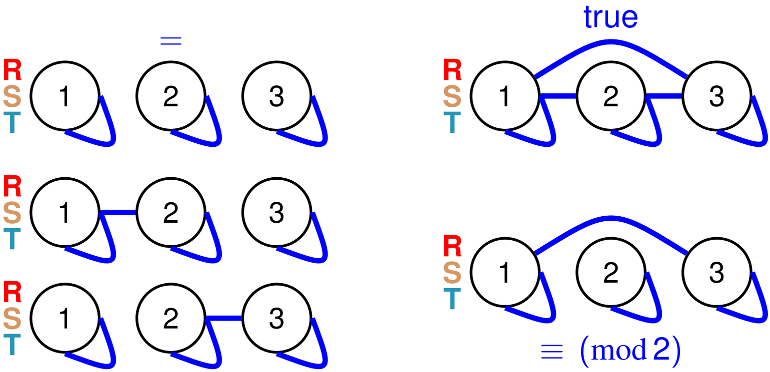
$$\textbf{Symmetric} \equiv \forall xy\, (E(x,y) \to E(y,x))$$

$$\textbf{Transitive} \equiv \forall xyz\, (E(x,y) \wedge E(y,z) \to E(x,z))$$



Equivalence Relations on 3-Element Sets

$$\textbf{Reflexive} \equiv \forall x\, E(x,x)$$
$$\textbf{Symmetric} \equiv \forall xy\, (E(x,y) \rightarrow E(y,x))$$
$$\textbf{Transitive} \equiv \forall xyz\, (E(x,y) \wedge E(y,z) \rightarrow E(x,z))$$

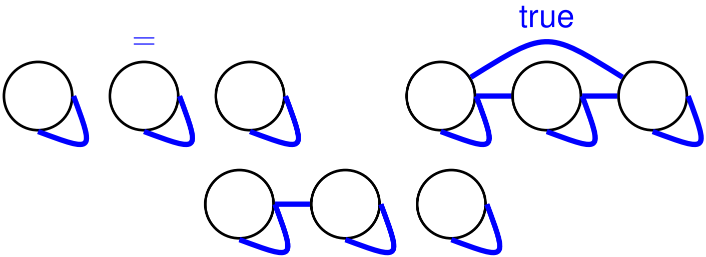


Equivalence Relations on 3-Element Sets

$$\textbf{Reflexive} \equiv \forall x\, E(x,x)$$

$$\textbf{Symmetric} \equiv \forall xy\,(E(x,y) \rightarrow E(y,x))$$

$$\textbf{Transitive} \equiv \forall xyz\,(E(x,y) \wedge E(y,z) \rightarrow E(x,z))$$



Partitions

Def. A **partition** of a non-empty set V is collection of pairwise disjoint, non-empty subsets, $(P_1, P_2, \ldots)$ of V whose union is V:

$$\emptyset \neq P_i \subseteq V \qquad P_i \cap P_j = \emptyset,\ i \neq j \qquad \bigcup P_i \ = \ V$$

Partitions

Def. A **partition** of a non-empty set V is collection of pairwise disjoint, non-empty subsets, $(P_1, P_2, \ldots)$ of V whose union is V:

$$\emptyset \neq P_i \subseteq V \qquad P_i \cap P_j = \emptyset,\ i \neq j \qquad \bigcup P_i \ = \ V$$

Prop. There are exactly five partitions of $V = \{1, 2, 3\}$:

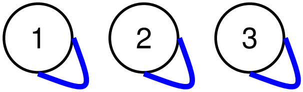
Partitions

Def. A **partition** of a non-empty set V is collection of pairwise disjoint, non-empty subsets, $(P_1, P_2, \ldots)$ of V whose union is V:

$$\emptyset \neq P_i \subseteq V \qquad P_i \cap P_j = \emptyset,\ i \neq j \qquad \bigcup P_i \ = \ V$$

Prop. There are exactly five partitions of $V = \{1, 2, 3\}$:

$(\{1\}, \{2\}, \{3\})$



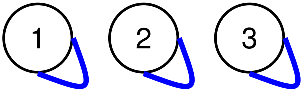
Partitions

Def. A **partition** of a non-empty set V is collection of pairwise disjoint, non-empty subsets, $(P_1, P_2, \ldots)$ of V whose union is V:

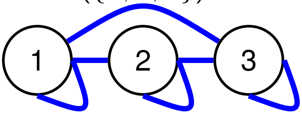
$$\emptyset \neq P_i \subseteq V \qquad P_i \cap P_j = \emptyset,\ i \neq j \qquad \bigcup P_i \ = \ V$$

Prop. There are exactly five partitions of $V = \{1, 2, 3\}$:

$(\{1\}, \{2\}, \{3\})$



$(\{1, 2, 3\})$



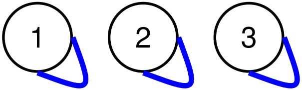
Partitions

Def. A **partition** of a non-empty set V is collection of pairwise disjoint, non-empty subsets, $(P_1, P_2, \ldots)$ of V whose union is V:

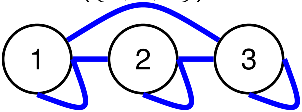
$$\emptyset \neq P_i \subseteq V \qquad P_i \cap P_j = \emptyset,\ i \neq j \qquad \bigcup P_i \ = \ V$$

Prop. There are exactly five partitions of $V = \{1, 2, 3\}$:

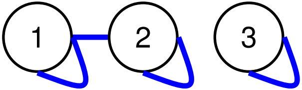
$(\{1\}, \{2\}, \{3\})$

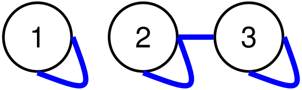


$(\{1, 2, 3\})$

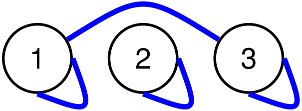


$(\{1, 2\}, \{3\})$





$(\{1\}, \{2, 3\})$



$(\{1, 3\}, \{2\})$

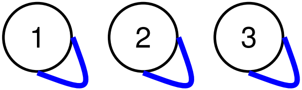
Partitions relate to Equivalence Relations, How?

Def. A **partition** of a non-empty set V is collection of pairwise disjoint, non-empty subsets, $(P_1, P_2, \ldots)$ of V whose union is V:

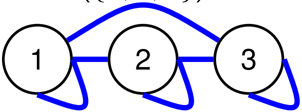
$$\emptyset \neq P_i \subseteq V \qquad P_i \cap P_j = \emptyset,\ i \neq j \qquad \bigcup P_i \ = \ V$$

Prop. There are exactly five partitions of $V = \{1, 2, 3\}$:

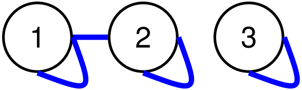
$(\{1\}, \{2\}, \{3\})$

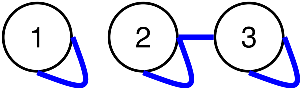


$(\{1, 2, 3\})$

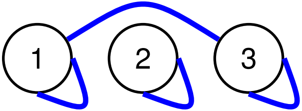


$(\{1, 2\}, \{3\})$





$(\{1\}, \{2, 3\})$



$(\{1, 3\}, \{2\})$

Thm. Let V be any nonempty set. Then there is a 1:1 correspondence, f_V, from Partitions on V to Equivalence Relations on V.

Thm. Let V be any nonempty set. Then there is a 1:1 correspondence, f_V, from Partitions on V to Equivalence Relations on V.

Proof: Let $P = (P_i), i \in I$ be a partition on V.

Thm. Let V be any nonempty set. Then there is a 1:1 correspondence, f_V, from Partitions on V to Equivalence Relations on V.

Proof: Let $P = (P_i), i \in I$ be a partition on V.

Let $p : V \to I$ be the function $p(v) \stackrel{\text{def}}{=}$ the unique $i \in I$, s.t. $v \in P_i$.

Thm. Let V be any nonempty set. Then there is a 1:1 correspondence, f_V, from Partitions on V to Equivalence Relations on V.

Proof: Let $P = (P_i), i \in I$ be a partition on V.

Let $p : V \to I$ be the function $p(v) \stackrel{\text{def}}{=}$ the unique $i \in I$, s.t. $v \in P_i$.

Let $x \equiv_P y$ iff $p(x) = p(y)$.

Thm. Let V be any nonempty set. Then there is a 1:1 correspondence, f_V, from Partitions on V to Equivalence Relations on V.

Proof: Let $P = (P_i), i \in I$ be a partition on V.

Let $p : V \to I$ be the function $p(v) \stackrel{\text{def}}{=}$ the unique $i \in I$, s.t. $v \in P_i$.

Let $x \equiv_P y$ iff $p(x) = p(y)$.

Observe that $\equiv_P$ is an equivalence relation on V.

Thm. Let V be any nonempty set. Then there is a 1:1 correspondence, f_V, from Partitions on V to Equivalence Relations on V.

Proof: Let $P = (P_i), i \in I$ be a partition on V.

Let $p : V \to I$ be the function $p(v) \stackrel{\text{def}}{=}$ the unique $i \in I$, s.t. $v \in P_i$.

Let $x \equiv_P y$ iff $p(x) = p(y)$.

Observe that $\equiv_P$ is an equivalence relation on V.

Conversely, let $\equiv$ be an Equivalence Relation on V.

Thm. Let V be any nonempty set. Then there is a 1:1 correspondence, f_V, from Partitions on V to Equivalence Relations on V.

Proof: Let $P = (P_i), i \in I$ be a partition on V.

Let $p : V \to I$ be the function $p(v) \stackrel{\text{def}}{=}$ the unique $i \in I$, s.t. $v \in P_i$.

Let $x \equiv_P y$ iff $p(x) = p(y)$.

Observe that $\equiv_P$ is an equivalence relation on V.

Conversely, let $\equiv$ be an Equivalence Relation on V.

Def. For any $v \in V$, let the **equivalence class** of v be

$$[v]_\equiv \quad \stackrel{\text{def}}{=} \quad \{w \in V \mid w \equiv v\}$$

Thm. Let V be any nonempty set. Then there is a 1:1 correspondence, f_V, from Partitions on V to Equivalence Relations on V.

Proof: Let $P = (P_i), i \in I$ be a partition on V.

Let $p : V \to I$ be the function $p(v) \stackrel{\text{def}}{=}$ the unique $i \in I$, s.t. $v \in P_i$.

Let $x \equiv_P y$ iff $p(x) = p(y)$.

Observe that $\equiv_P$ is an equivalence relation on V.

Conversely, let $\equiv$ be an Equivalence Relation on V.

Def. For any $v \in V$, let the **equivalence class** of v be

$$[v]_\equiv \quad \stackrel{\text{def}}{=} \quad \{w \in V \mid w \equiv v\}$$

Observe that the set of distinct equivalence classes, $([v]_\equiv), v \in V$, is a partition. □

Thm. For all $m > 1$, $x \equiv y \pmod{m}$ is an Equivalence Relation.

Thm. For all $m > 1$, $x \equiv y \pmod{m}$ is an Equivalence Relation.

Proof: R27 Reading Quiz $\square$

Thm. For all $m > 1$, $x \equiv y \pmod{m}$ is an Equivalence Relation.

Proof: R27 Reading Quiz □

Thm. For all $m > 1$ and for all $a, a', b, b', n \in \mathbf{Z}$ if $a \equiv a' \pmod{m}$ and $b \equiv b' \pmod{m}$ then

Thm. For all $m > 1$, $x \equiv y \pmod{m}$ is an Equivalence Relation.

Proof: R27 Reading Quiz $\square$

Thm. For all $m > 1$ and for all $a, a', b, b', n \in \mathbf{Z}$ if $a \equiv a' \pmod{m}$ and $b \equiv b' \pmod{m}$ then

1. $a + b \equiv a' + b' \pmod{m}$

Thm. For all $m > 1$, $x \equiv y \pmod{m}$ is an Equivalence Relation.

Proof: R27 Reading Quiz □

Thm. For all $m > 1$ and for all $a, a', b, b', n \in \mathbf{Z}$ if $a \equiv a' \pmod{m}$ and $b \equiv b' \pmod{m}$ then

1. $a + b \equiv a' + b' \pmod{m}$
2. $a \cdot b \equiv a' \cdot b' \pmod{m}$

Thm. For all $m > 1$, $x \equiv y \pmod{m}$ is an Equivalence Relation.

Proof: R27 Reading Quiz □

Thm. For all $m > 1$ and for all $a, a', b, b', n \in \mathbf{Z}$ if $a \equiv a' \pmod{m}$ and $b \equiv b' \pmod{m}$ then

1. $a + b \equiv a' + b' \pmod{m}$
2. $a \cdot b \equiv a' \cdot b' \pmod{m}$
3. $a^n \equiv (a')^n \pmod{m}$

Recall L17: $a^{-1} \bmod m$ exists iff $\gcd(a, m) = 1$

$\cdot \mathbb{Z}/6\mathbb{Z}$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

Recall L17: $a^{-1} \bmod m$ exists iff $\gcd(a, m) = 1$

$\cdot Z/6Z$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

Def. $\mathbf{Z}_m^*$ is the **multiplicative group mod m**.

Recall L17: $a^{-1} \bmod m$ exists iff $\gcd(a, m) = 1$

$\cdot_{Z/6Z}$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

Def. $\mathbf{Z}_m^*$ is the **multiplicative group mod m**.

$$|\mathbf{Z}_m^*| = \{a \in \mathbf{Z}/m\mathbf{Z} \mid \gcd(a, m) = 1\} \qquad x \cdot_{Z_m^*} y = (x \cdot y) \,\%\, m$$

Recall L17: $a^{-1} \bmod m$ exists iff $\gcd(a, m) = 1$

$\cdot_{Z/6Z}$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

Def. $\mathbf{Z}_m^*$ is the **multiplicative group mod m**.

$$|\mathbf{Z}_m^*| = \{a \in \mathbf{Z}/m\mathbf{Z} \mid \gcd(a, m) = 1\} \qquad x \cdot_{Z_m^*} y = (x \cdot y) \,\%\, m$$

$$|\mathbf{Z}_6^*| = \{1, 5\}$$

$\cdot_{Z_6^*}$	1	5
1	1	5
5	5	1

$\mathbf{Z}_m^*$ is the multiplicative group mod m

$$|\mathbf{Z}_5^\star| = \{1, 2, 3, 4\}$$

$\cdot Z_5^\star$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

Groups

$$\Sigma_{\mathsf{group}} \stackrel{\text{def}}{=} (;\mathsf{1}, \cdot[\text{infix}]^{\mathsf{2}}, {}^{-1}[\text{postfix}]^{\mathsf{1}})$$

Groups

$$\Sigma_{\text{group}} \stackrel{\text{def}}{=} (;1, \cdot[\text{infix}]^2, ^{-1}[\text{postfix}]^1)$$

$$G_1 \quad = \quad \forall x\, y\, z \quad x \cdot (y \cdot z) \;=\; (x \cdot y) \cdot z \qquad\qquad \textit{associative}$$

Groups

$$\Sigma_{\mathsf{group}} \stackrel{\text{def}}{=} (;1, \cdot[\text{infix}]^2, ^{-1}[\text{postfix}]^1)$$

$$G_1 = \forall x\, y\, z \quad x \cdot (y \cdot z) = (x \cdot y) \cdot z \qquad \textit{associative}$$

$$G_2 = \forall x \quad x \cdot 1 = x \qquad \textit{identity}$$

Groups

$$\Sigma_{\text{group}} \stackrel{\text{def}}{=} (;1, \cdot[\text{infix}]^2, {}^{-1}[\text{postfix}]^1)$$

$$G_1 = \forall x\, y\, z \quad x \cdot (y \cdot z) = (x \cdot y) \cdot z \qquad \textit{associative}$$

$$G_2 = \forall x \quad x \cdot 1 = x \qquad \textit{identity}$$

$$G_3 = \forall x \quad x \cdot x^{-1} = 1 \qquad \textit{inverses}$$

Groups

$$\Sigma_{\text{group}} \stackrel{\text{def}}{=} (; 1, \cdot[\text{infix}]^2, ^{-1}[\text{postfix}]^1)$$

$$
\begin{array}{lcll}
G_1 & = & \forall x\, y\, z \quad x \cdot (y \cdot z) = (x \cdot y) \cdot z & \textit{associative} \\
G_2 & = & \forall x \quad x \cdot 1 = x & \textit{identity} \\
G_3 & = & \forall x \quad x \cdot x^{-1} = 1 & \textit{inverses}
\end{array}
$$

Def. A **group** is a $G \in \text{World}[\Sigma_{\text{group}}]$ s.t. $G \models G_1 \wedge G_2 \wedge G_3$.

Groups

$$\Sigma_{\text{group}} \stackrel{\text{def}}{=} (;1, \cdot[\text{infix}]^2, ^{-1}[\text{postfix}]^1)$$

$$\begin{array}{lcll} G_1 & = & \forall x\, y\, z \quad x \cdot (y \cdot z) = (x \cdot y) \cdot z & \textit{associative} \\ G_2 & = & \forall x \quad x \cdot 1 = x & \textit{identity} \\ G_3 & = & \forall x \quad x \cdot x^{-1} = 1 & \textit{inverses} \end{array}$$

Def. A **group** is a $G \in \text{World}[\Sigma_{\text{group}}]$ s.t. $G \models G_1 \wedge G_2 \wedge G_3$.

Prop. For all $m > 1$, Z_m^* is a group.

Euler's phi function, φ

Def. For $m > 1$,

$$\varphi(m) \stackrel{\text{def}}{=} \|\mathbf{Z}_m^*\| = \left|\{a \in \mathbf{Z}/m\mathbf{Z} \mid \gcd(a, m) = 1\}\right|$$

m	$\varphi(m)$	$\lvert\mathbf{Z}_m^*\rvert$
2	1	$\{1\}$
3	2	$\{1, 2\}$
4	2	$\{1, 3\}$
5	4	$\{1, 2, 3, 4\}$
6	2	$\{1, 5\}$
7	6	$\{1, 2, 3, 4, 5, 6\}$
8	4	$\{1, 3, 5, 7\}$
9	6	$\{1, 2, 4, 5, 7, 8\}$
10	4	$\{1, 3, 7, 9\}$
11	10	$\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$
12	4	$\{1, 5, 7, 11\}$

Fermat's Little Theorem

Thm: For p prime, $a \in \mathbf{Z}_p^\star$, $a^{p-1} \equiv 1 \pmod{p}$

Proof:

$f_a : \mathbf{Z}_p^\star \underset{\text{onto}}{\overset{1:1}{\rightarrow}} \mathbf{Z}_p^\star$; $\quad f_a(x) = (a \cdot x) \quad f_a^{-1}(x) = ((a^{-1} (\bmod p)) \cdot x)$

Fermat's Little Theorem

Thm: For p prime, $a \in \mathbf{Z}_p^\star$, $a^{p-1} \equiv 1 \pmod{p}$

Proof:

$f_a : \mathbf{Z}_p^\star \underset{\text{onto}}{\overset{1:1}{\rightarrow}} \mathbf{Z}_p^\star$; $\quad f_a(x) = (a \cdot x) \quad f_a^{-1}(x) = ((a^{-1} (\bmod p)) \cdot x)$

$$Z_p^\star = \{1, 2, \ldots, p-1\} \quad = \quad \{f_a(1), f_a(2), \ldots, f_a(p-1)\}$$

Fermat's Little Theorem

Thm: For p prime, $a \in \mathbf{Z}_p^\star$, $a^{p-1} \equiv 1 \pmod{p}$

Proof:

$f_a : \mathbf{Z}_p^\star \underset{\text{onto}}{\overset{1:1}{\rightarrow}} \mathbf{Z}_p^\star$; $\quad f_a(x) = (a \cdot x) \quad f_a^{-1}(x) = ((a^{-1} (\bmod p)) \cdot x)$

$$Z_p^\star = \{1, 2, \ldots, p-1\} = \{f_a(1), f_a(2), \ldots, f_a(p-1)\}$$

$$\{1, 2, \ldots, p-1\} = \{a \cdot 1, a \cdot 2, \ldots, a \cdot (p-1)\}$$

Fermat's Little Theorem

Thm: For p prime, $a \in \mathbf{Z}_p^\star$, $a^{p-1} \equiv 1 \pmod p$

Proof:

$f_a : \mathbf{Z}_p^\star \overset{1:1}{\underset{\text{onto}}{\rightarrow}} \mathbf{Z}_p^\star$; $\quad f_a(x) = (a \cdot x) \quad f_a^{-1}(x) = ((a^{-1}(\bmod p)) \cdot x)$

$$Z_p^\star = \{1, 2, \ldots, p-1\} = \{f_a(1), f_a(2), \ldots, f_a(p-1)\}$$

$$\{1, 2, \ldots, p-1\} = \{a \cdot 1, a \cdot 2, \ldots, a \cdot (p-1)\}$$

$$\prod_{i \in \mathbf{Z}_p^\star} i \equiv \prod_{i \in \mathbf{Z}_p^\star} a \cdot i \pmod p$$

Fermat's Little Theorem

Thm: For p prime, $a \in \mathbf{Z}_p^\star$, $a^{p-1} \equiv 1 \pmod p$

Proof:

$f_a : \mathbf{Z}_p^\star \underset{\text{onto}}{\overset{1:1}{\rightarrow}} \mathbf{Z}_p^\star; \quad f_a(x) = (a \cdot x) \quad f_a^{-1}(x) = ((a^{-1}(\bmod p)) \cdot x)$

$$Z_p^\star = \{1, 2, \ldots, p-1\} = \{f_a(1), f_a(2), \ldots, f_a(p-1)\}$$

$$\{1, 2, \ldots, p-1\} = \{a \cdot 1, a \cdot 2, \ldots, a \cdot (p-1)\}$$

$$\prod_{i \in \mathbf{Z}_p^\star} i \equiv \prod_{i \in \mathbf{Z}_p^\star} a \cdot i \pmod p$$

$$\prod_{i \in \mathbf{Z}_p^\star} i \equiv a^{p-1} \prod_{i \in \mathbf{Z}_p^\star} i \pmod p$$

Fermat's Little Theorem

Thm: For p prime, $a \in \mathbf{Z}_p^\star$, $a^{p-1} \equiv 1 \pmod{p}$

Proof:

$f_a : \mathbf{Z}_p^\star \underset{\text{onto}}{\overset{1:1}{\rightarrow}} \mathbf{Z}_p^\star; \quad f_a(x) = (a \cdot x) \quad f_a^{-1}(x) = ((a^{-1} (\bmod p)) \cdot x)$

$$Z_p^\star = \{1, 2, \ldots, p-1\} = \{f_a(1), f_a(2), \ldots, f_a(p-1)\}$$

$$\{1, 2, \ldots, p-1\} = \{a \cdot 1, a \cdot 2, \ldots, a \cdot (p-1)\}$$

$$\prod_{i \in \mathbf{Z}_p^\star} i \equiv \prod_{i \in \mathbf{Z}_p^\star} a \cdot i \pmod{p}$$

$$\prod_{i \in \mathbf{Z}_p^\star} i \equiv a^{p-1} \prod_{i \in \mathbf{Z}_p^\star} i \pmod{p}$$

$$1 \equiv a^{p-1} \pmod{p} \qquad \square$$