More on Relations 1

Wolfgang Schreiner
Research Institute for Symbolic Computation (RISC-Linz)
Johannes Kepler University, Linz, Austria

Wolfgang.Schreiner@risc.uni-linz.ac.at
http://www.risc.uni-linz.ac.at/people/schreine

Equivalence Relations and Partitions

Overview

- Equivalence Relations and Partitions
- Modular Arithmetic
- Another Construction of Number Domains

Relation Properties

Definition: A binary relation R on a set S is reflexive, symmetric, respectively transitive, if it satisfies the following properties:

$$
\begin{array}{l}
R \text{ is reflexive on } S :\Leftrightarrow \\
\quad \forall x \in S : \langle x, x \rangle \in R; \\
R \text{ is symmetric on } S :\Leftrightarrow \\
\quad \forall x, y : \langle x, y \rangle \in R \Rightarrow \langle y, x \rangle \in R; \\
R \text{ is transitive on } S :\Leftrightarrow \\
\quad \forall x, y, z : (\langle x, y \rangle \in R \land \langle y, z \rangle \in R) \Rightarrow \langle x, z \rangle \in R.
\end{array}
$$

Example: equality is reflexive, symmetric and transitive on every set.

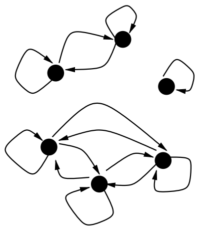
Equivalence Relation

Definition: Let R be a binary relation on S. R is an equivalence relation on S, if it is reflexive, symmetric, and transitive on S:

$$\begin{aligned}&R \text{ is equivalence relation on } S :\Leftrightarrow\\ &\quad R \subseteq S \times S \wedge\\ &\quad R \text{ is reflexive on } S \wedge\\ &\quad R \text{ is symmetric on } S \wedge\\ &\quad R \text{ is transitive on } S.\end{aligned}$$

Many (not all) properties of the equality relation on S.

Visualization



- Reflexivity: every node has an arrow to itself,
- Symmetry: if there is an arrow from node a to node b, then there is also an arrow from b to a,
- Transitivity: if there is an arrow from node a to node b and an arrow from b to some node c, then there is an arrow from a to c.

Example

- $p(x, y) :\Leftrightarrow x + y$ is even

  Equivalence relation on $\mathbb{N}$.
- $r(x, y) :\Leftrightarrow x_0 + y_1 = x_1 + y_0$

  Equivalence relation on $\mathbb{R} \times \mathbb{R}$.
- $s(x, y) :\Leftrightarrow x$ is parallel to (or coincides with) y

  Equivalence relation on the set of all lines in the plane.
- $t(x, y) :\Leftrightarrow x$ has the same age as y

  Equivalence relation on the set of all people.

Proof

We prove $p(x, y) :\Leftrightarrow x + y$ is even is an equivalence relation on $\mathbb{N}$.

1. p is clearly a binary relation on $\mathbb{N}$.
2. p is reflexive on $\mathbb{N}$: Take arbitrary $x \in \mathbb{N}$. We have to show $x + x$ is even, i.e, $2x$ is even.
3. p is symmetric on $\mathbb{N}$: Take $x \in \mathbb{N}$, $y \in \mathbb{N}$. We assume $x + y$ is even. Then $y + x$ is even.
4. p is transitive on $\mathbb{N}$: Take arbitrary $x \in \mathbb{N}$, $y \in \mathbb{N}$, and $z \in \mathbb{N}$. We assume

   $$(1)\ x + y \text{ is even} \wedge y + z \text{ is even.}$$

   We have to show $(2)\ x + z$ is even. From (1), we have some $a \in \mathbb{N}$ and $b \in \mathbb{N}$ such that

   $$(3)\ 2a = x + y \wedge 2b = y + z.$$

   Thus we know (2) because of

   $$x + z = (x + y) + (y + z) - 2y = 2a + 2b - 2y = 2(a + b - y).$$

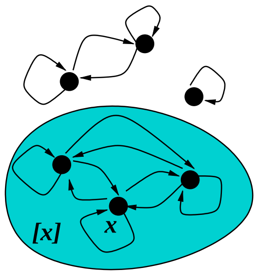
Class

Definition: The class of x with respect to R is the set of all elements that are related to x by R:

$$[x]_R := \{y \in \mathrm{range}(R) : \langle x, y\rangle \in R\}.$$

- We may just write $[x]$, if R is clear from the context.
- If R is an equivalence relation, we call $[x]_R$ the equivalence class of x with respect to R.

Visualization



The equivalence class of a node x is the set of all nodes to which x is (directly or indirectly) connected.

Example

Let $p \subseteq \mathbb{N} \times \mathbb{N}$ such that $p(x, y) \Leftrightarrow x + y \text{ is even.}$ Then we have

$$\begin{aligned}
[0]_p &= \{0, 2, 4, 6, 8, 10, \ldots\},\\
[1]_p &= \{1, 3, 5, 7, 9, 11, \ldots\},\\
[2]_p &= \{0, 2, 4, 6, 8, 10, \ldots\},\\
[3]_p &= \{1, 3, 5, 7, 9, 11, \ldots\},\\
[4]_p &= \{0, 2, 4, 6, 8, 10, \ldots\},\\
&\ldots
\end{aligned}$$

We see that $[0]_p \cup [1]_p = \mathbb{N}$ and $[0]_p \cap [1]_p = \emptyset$.

Example

Let $q \subseteq \mathbb{N} \times \mathbb{N}$ such that $q(x, y) \Leftrightarrow x \bmod 5 = \mathrm{y} \bmod 5.$ We have

$$\begin{aligned}
[0]_q &= \{0, 5, 10, 15, 20, 25, \ldots\},\\
[1]_q &= \{1, 6, 11, 16, 21, 26, \ldots\},\\
[2]_q &= \{2, 7, 12, 17, 22, 27, \ldots\},\\
[3]_q &= \{3, 8, 13, 18, 23, 28, \ldots\},\\
[4]_q &= \{4, 9, 14, 19, 24, 29, \ldots\},\\
[5]_q &= \{0, 5, 10, 15, 20, 25, \ldots\},\\
&\ldots
\end{aligned}$$

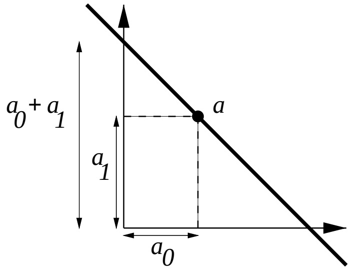
We see that $[0]_q \cup [1]_q \cup [2]_q \cup [3]_q \cup [4]_q = \mathbb{N}$ and that any two of these sets are disjoint.

Example

Let $r \subseteq (\mathbb{R} \times \mathbb{R}) \times (\mathbb{R} \times \mathbb{R})$ such that $r(x, y) \Leftrightarrow x_0 + x_1 = y_0 + y_1$.

$$[a]_r = \{b \in \mathbb{R} \times \mathbb{R} : a_0 + a_1 = b_0 + b_1\}$$
$$[a]_r = \{b \in \mathbb{R} \times \mathbb{R} : b_1 = -b_0 + (a_0 + a_1)\}$$

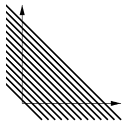
$[a]_r$ denotes the line with slope -1 that goes through a:



Example (Continued)

$$\mathbb{R} \times \mathbb{R} = \bigcup_{a \in \mathbb{R} \times \mathbb{R}} [a]_r$$

The plane is partitioned into the set of all these lines:



We can determine a "canonical representative" for each such line:

$$\mathbb{R} \times \mathbb{R} = \bigcup_{y \in \mathbb{R}} [\langle 0, y \rangle]_r$$

Class Properties

Proposition: Let R be an equivalence relation on S. $[x]_R$ contains x, for every $x \in S$:

$$\forall S, R : R \text{ is equivalence relation on } S \Rightarrow \forall x \in S : x \in [x]_R.$$

Let x and y be elements of S. The equivalence classes of x and y with respect to R are either identical or disjoint:

$$\begin{array}{l} \forall S, R : R \text{ is equivalence relation on } S \Rightarrow \\ \quad \forall x \in S, y \in S : \\ \quad\quad [x]_R = [y]_R \vee [x]_R \cap [y]_R = \emptyset. \end{array}$$

Quotient Set

Definition: The quotient set of S with respect to R is the set of all classes induced on S by R:

$$S/R := \{[x]_R : x \in S\}.$$

By class properties, every set S is partitioned by an equivalence relation R into a set of non-empty and disjoint subsets (blocks).

Partition

Definition: D is a partition or decomposition of S, if its elements, the blocks, are non-empty and disjoint and their union equals S:

$$\begin{aligned}&D \text{ is partition of } S :\Leftrightarrow \\ &\quad (\forall x \in D : x \neq \emptyset) \wedge \\ &\quad (\forall x \in D, y \in D : x = y \vee x \cap y = \emptyset) \wedge \\ &\quad \bigcup D = S.\end{aligned}$$

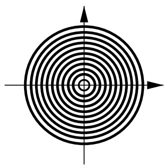
Example

- The set $\{A, B, C\}$ is a partition of $\mathbb{N}$.

$$\begin{aligned}A &:= \{x \in \mathbb{N} : x \text{ is even}\},\\ B &:= \{x \in \mathbb{N} : x > 2 \wedge x \text{ is prime}\},\\ C &:= \{x \in \mathbb{N} : x \text{ is odd} \wedge x \text{ is not prime}\}.\end{aligned}$$

- The set $\{\text{circle}(r) : r \in \mathbb{R}_{\geq 0}\}$ is a partition of $\mathbb{R} \times \mathbb{R}$.

$$\text{circle}(r) := \{p \in \mathbb{R} \times \mathbb{R} : {p_0}^2 + {p_1}^2 = r^2\}.$$



Equivalence Relations and Partitions

Proposition: Let R be an equivalence relation on S. The quotient set of S with respect to R is a partition of S:

$$\begin{aligned}&\forall S, R : R \text{ is equivalence relation on } S \;\Rightarrow \\ &\quad S/R \text{ is partition of } S.\end{aligned}$$

Proof: see lecture notes.

Every equivalence relation defines a partition.

Partitions and Equivalence Relations

Definition: The relation induced by a partition D is the set of all pairs of elements of the same block of D:

$$x \sim_D y :\Leftrightarrow \exists d \in D : x \in d \wedge y \in d.$$

Proposition: Let D be a partition of S. The relation induced by D is an equivalence relation on S:

$$\begin{aligned}&\forall S, D : D \text{ is partition of } S \;\Rightarrow \\ &\quad \sim_D \text{ is equivalence relation on } S.\end{aligned}$$

Every partition defines an equivalence relation.

Relationship between Constructions

Proposition: Let R be an equivalence relation on S. Then R is the relation induced by the quotient set of S with respect to R:

$$\forall S, R : R \text{ is equivalence relation on } S \Rightarrow \\ R = \sim_{S/R} .$$

Let D be a partition of S. Then D is the quotient set of the relation induced by D:

$$\forall S, D : D \text{ is partition of } S \Rightarrow \\ D = S/\sim_D .$$

Each construction is the inverse of the other.

Modular Arithmetic

Motivation

- $\mathbb{Z}$ has infinite size.

  Infinitely many integers, no upper bound.

- Computer processors can only operate with finite subset.

  On a 64 bit processor, only 2^{64} integers, upper bound 2^{32}.

- How deal with operation "overflows"?

$$2^{20} * 2^{30} = ?$$

Need domain for modeling processor arithmetic.

Direct Approach

Definition: Let $m \in \mathbb{Z}_{>0}$ and $\mathbb{Z}_m := \{x \in \mathbb{Z} : 0 \leq x < m\}$.

$$+_m : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}_m \\ x +_m y := (x + y) \bmod m$$

$$-_m : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}_m \\ -_m x := (-x) \bmod m$$

$$*_m : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}_m \\ x *_m y := (x * y) \bmod m$$

Example

Arithmetic modulo 3:

$+_3$	-4	-3	-2	-1	0	1	2	3	4
-4	1	2	0	1	2	0	1	2	0
-3	2	0	1	2	0	1	2	0	1
-2	0	1	2	0	1	2	0	1	2
-1	1	2	0	1	2	0	1	2	0
0	2	0	1	2	0	1	2	0	1
1	0	1	2	0	1	2	0	1	2
2	1	2	0	1	2	0	1	2	0
3	2	0	1	2	0	1	2	0	1
4	0	1	2	0	1	2	0	1	2

$*_3$	-4	-3	-2	-1	0	1	2	3	4
-4	1	0	2	1	0	2	1	0	2
-3	0	0	0	0	0	0	0	0	0
-2	2	0	1	2	0	1	2	0	1
-1	1	0	2	1	0	2	1	0	2
0	0	0	0	0	0	0	0	0	0
1	2	0	1	2	0	1	2	0	1
2	1	0	2	1	0	2	1	0	2
3	0	0	0	0	0	0	0	0	0
4	2	0	1	2	0	1	2	0	1

Same pattern is repeated every 3 lines and every 3 columns.

Observation

- Same pattern repeated every m lines and every m columns.
- Does not matter whether we compute with a or with

  $a + m$,
  $a - m$,
  $a + im$, for any $i \in \mathbb{Z}$.
- The elements of the set

  $$[a]_m := \{a + im : i \in \mathbb{Z}\}$$

  cannot be distinguished from a by arithmetic modulo m.

Can define modular arithmetic by equivalence classes.

Modular Congruence

Definition: Two integers x and y are congruent modulo m if they have the same remainder when divided by m:

$$x \equiv_m y :\Leftrightarrow (x \bmod m) = (y \bmod m).$$

Proposition: $\equiv_m$ is an equivalence relation, for every $m \in \mathbb{Z}_{>0}$.

Residue Class

Definition: The residue class of a modulo m is the set of all integer numbers that are congruent to a modulo m.

$$[a]_m := [a]_{\equiv_m}.$$

Proposition: $[a]_m = \{a + im : i \in \mathbb{Z}\}$, for every $a \in \mathbb{Z}, m \in \mathbb{Z}_{>0}$.

- $\equiv_m$ defines the $[a]_m$ of our intuition.
- $\equiv_m$ also defines a suitable domain $\mathbb{Z}_m$ for modular arithmetic.

Modular Integer Numbers

Definition: The set of integers modulo m is the quotient set of $\mathbb{Z}$ with respect to congruence modulo m:

$$\mathbb{Z}_m := \mathbb{Z}/\equiv_m .$$

Proposition: $\mathbb{Z}_m$ has m elements each of which is represented by a natural number less than m, i.e.,

$$\mathbb{Z}_m = \{[0]_m, [1]_m, [2]_m, \ldots, [m-1]_m\}.$$

Congruence Properties

Proposition: Let a and a' be in the same residue class and also b and b' be in the same residue class. The result of any integer operation involving a and b is in the same residue class as if the operation were performed with a' and b' instead:

$$\begin{array}{l}\forall m \in \mathbb{Z}_{>0}, a \in \mathbb{Z}, a' \in \mathbb{Z}, b \in \mathbb{Z}, b' \in \mathbb{Z} : \\ \quad [a]_m = [a']_m \wedge [b]_m = [b']_m \ \Rightarrow \\ \qquad [a+b]_m = [a'+b']_m \ \wedge \\ \qquad [-a]_m = [-a']_m \ \wedge \\ \qquad [a*b]_m = [a'*b']_m.\end{array}$$

Example

We have $[7]_5 = [2]_5$ and $[9]_5 = [4]_5$. Consequently,

$$[7+9]_5 = [2+4]_5 = [6]_5 = [1]_5.$$

When dealing with e.g.

$$[3]_5 = \{\ldots, -7, -2, 3, 8, 13, \ldots\}$$

we need not take the "canonical" representative 3 but may also choose -2 or 8 as the representative for computation.

Modular Arithmetic

Let $m \in \mathbb{Z}_{>0}$ and define the selector function

$$\overline{x} := \textbf{such } a \in \mathbb{Z} : x = [a]_m.$$

$$\begin{array}{l} +_m : \mathbb{Z}_m \times \mathbb{Z}_m \to \mathbb{Z}_m \\ x +_m y := [\overline{x} +_{\mathbb{Z}} \overline{y}]_m \end{array}$$

$$\begin{array}{l} -_m : \mathbb{Z}_m \to \mathbb{Z}_m \\ -_m\, x := [-_{\mathbb{Z}}\, \overline{x}]_m \end{array}$$

$$\begin{array}{l} *_m : \mathbb{Z}_m \times \mathbb{Z}_m \to \mathbb{Z}_m \\ x *_m y := [\overline{x} *_{\mathbb{Z}} \overline{y}]_m \end{array}$$

Equivalent Definition

$$
\begin{aligned}
&+_m : \mathbb{Z}_m \times \mathbb{Z}_m \to \mathbb{Z}_m \\
&[a]_m +_m [b]_m := [a +_{\mathbb{Z}} b]_m \\[1em]
&-_m : \mathbb{Z}_m \to \mathbb{Z}_m \\
&-_m[a]_m := [-_{\mathbb{Z}}\, a]_m \\[1em]
&*_m : \mathbb{Z}_m \times \mathbb{Z}_m \to \mathbb{Z}_m \\
&[a]_m *_m [b]_m := [a *_{\mathbb{Z}} b]_m
\end{aligned}
$$

Because of congruence properties, functions are uniquely defined.

Operational Interpretation

For performing arithmetic on some $x \in \mathbb{Z}_m$,

1. we apply the selector function to determine a representative $\overline{x} \in \mathbb{Z}$,
2. perform the corresponding operation in $\mathbb{Z}$ to yield the result $r \in \mathbb{Z}$,
3. and then determine the residue class $[r]_m \in \mathbb{Z}_m$.

Because of congruence, choice of the representative does not matter.

Example

We consider arithmetic in $\mathbb{Z}_5 = \{[0]_5, [1]_5, [2]_5, [3]_5, [4]_5\}$.

$$
\begin{aligned}
[17]_5 +_5 [24]_5 &= [2]_5 +_5 [4]_5 = [6]_5 = [1]_5 \\
[7]_5 -_5 [10]_5 &= [2]_5 -_5 [0]_5 = [3]_5 \\
[-7]_5 &= [3]_5 \\
[6]_5 *_5 [9]_5 &= [1]_5 *_5 [4]_5 = [4]_5 \\
[-3]_5 *_5 [6]_5 &= [2]_5 *_5 [1]_5 = [2]_5
\end{aligned}
$$

Another Construction of Number Domains

Direct Definition of Integer Numbers

- Integer as a tuple $\langle x, y\rangle$.
- Difference between x and y denotes desired value.
- For unique definition, x or y is chosen 0.
- Constructor fuction I to build well-formed integers.

More elegant: integer as <u>class</u> of all $\langle x, y\rangle$ with same difference.

Integer Domain

Definition: Set of integer numbers $\mathbb{Z}$:

$$x \sim_{\mathbb{Z}} y :\Leftrightarrow (x_0 +_{\mathbb{N}} y_1 = y_0 +_{\mathbb{N}} x_1)$$

$$\mathbb{Z} := (\mathbb{N} \times \mathbb{N}) / \sim_{\mathbb{Z}}$$

Partitioning of $\mathbb{N} \times \mathbb{N}$ by equivalence relation.

Integer Arithmetic

$$0 := [\langle 0_{\mathbb{N}}, 0_{\mathbb{N}}\rangle];\ \ 1 := [\langle 1_{\mathbb{N}}, 0_{\mathbb{N}}\rangle];\ \ 2 := [\langle 2_{\mathbb{N}}, 0_{\mathbb{N}}\rangle]$$

$$\overline{x} := \textbf{such } a \in \mathbb{N} \times \mathbb{N} : x = [a]$$

$$\begin{aligned}
x + y &:= [\langle \overline{x}_0 +_{\mathbb{N}} \overline{y}_0, \overline{x}_1 +_{\mathbb{N}} \overline{y}_1\rangle] \\
-x &:= [\langle \overline{x}_1, \overline{x}_0\rangle] \\
x - y &:= [\langle \overline{x}_0 +_{\mathbb{N}} \overline{y}_1, \overline{y}_0 +_{\mathbb{N}} \overline{x}_1\rangle] \\
x * y &:= [\langle (\overline{x}_0 *_{\mathbb{N}} \overline{y}_0) +_{\mathbb{N}} (\overline{x}_1 *_{\mathbb{N}} \overline{y}_1), (\overline{x}_0 *_{\mathbb{N}} \overline{y}_1) +_{\mathbb{N}} (\overline{x}_1 *_{\mathbb{N}} \overline{y}_0)\rangle] \\
x \leq y &:\Leftrightarrow \overline{x}_0 + \overline{y}_1 \leq_{\mathbb{N}} \overline{y}_0 + \overline{x}_1
\end{aligned}$$

Since $\sim_{\mathbb{Z}}$ is a congruence relation, functions are uniquely defined.

Example

$$\begin{aligned}
5 &= [\langle 7, 2\rangle] = \{\langle 5, 0\rangle, \langle 6, 1\rangle, \langle 7, 2\rangle, \langle 8, 3\rangle, \ldots\} \\
-6 &= [\langle 3, 9\rangle] = \{\langle 0, 6\rangle, \langle 1, 7\rangle, \langle 2, 8\rangle, \langle 3, 9\rangle, \ldots\} \\
5 + (-6) &= [\langle 7, 2\rangle] + [\langle 3, 9\rangle] = [\langle 10, 11\rangle] = [\langle 0, 1\rangle] = -1 \\
5 * (-6) &= [\langle 7, 2\rangle] * [\langle 3, 9\rangle] = [\langle 39, 69\rangle] = [\langle 0, 30\rangle] = -30 \\
5 \leq -6 &\Leftrightarrow [\langle 7, 2\rangle] \leq [\langle 3, 9\rangle] \Leftrightarrow 16 \leq 5 \Leftrightarrow \mathrm{F}.
\end{aligned}$$

Isomorphism of Integer Constructions

Proposition: Let $\mathbb{Z}$' denote the old construction of the integers and $\mathbb{Z}$ denote the new one. The function $i : \mathbb{Z}' \rightarrow \mathbb{Z}$

$$i(x) := [x]$$

is an isomorphism with respect to $0, +, -, *, <$, i.e., i is bijective and for all $x \in \mathbb{Z}'$ and $y \in \mathbb{Z}'$, we have:

$$\begin{array}{rcl} i(0_{\mathbb{Z}'}) & = & 0_{\mathbb{Z}}, \\ i(x +_{\mathbb{Z}'} y) & = & i(x) +_{\mathbb{Z}} i(y), \\ i(-_{\mathbb{Z}'} x) & = & -_{\mathbb{Z}}\, i(x), \\ i(x -_{\mathbb{Z}'} y) & = & i(x) -_{\mathbb{Z}} i(y), \\ \ldots & & \end{array}$$

Inverse Isomorphism: $j : \mathbb{Z} \rightarrow \mathbb{Z}'$, $j(x) := \mathrm{I}(\overline{x})$

Rational Numbers

Definition: Set of rational numbers $\mathbb{Q}$:

$$x \sim_{\mathbb{Q}} y :\Leftrightarrow (x_0 *_{\mathbb{Z}} y_1 = y_0 *_{\mathbb{Z}} x_1)$$

$$\mathbb{Q} := (\mathbb{Z} \times \mathbb{Z}_{\neq 0}) / \sim_{\mathbb{Q}}$$

Arithmetic: see lecture notes.

Isomorphism of Rational Constructions

Proposition: Let $\mathbb{Q}$' denote the old construction of the integers and $\mathbb{Q}$ denote the new one. The function $i : \mathbb{Q}' \rightarrow \mathbb{Q}$

$$i(x) := [x]$$

is an isomorphism with respect to $0, +, -, *, ', <$, i.e., i is bijective and for all $x \in \mathbb{Q}'$ and $y \in \mathbb{Q}'$, we have:

$$\begin{array}{rcl} i(0_{\mathbb{Q}'}) & = & 0_{\mathbb{Q}}, \\ i(x +_{\mathbb{Q}'} y) & = & i(x) +_{\mathbb{Q}} i(y), \\ i(-_{\mathbb{Q}'} x) & = & -_{\mathbb{Q}}\, i(x), \\ i(x -_{\mathbb{Q}'} y) & = & i(x) -_{\mathbb{Q}} i(y), \\ \ldots & & \end{array}$$

Inverse Isomorphism: $j : \mathbb{Q} \rightarrow \mathbb{Q}'$, $j(x) := \frac{\overline{x}_0}{\overline{x}_1}$.

Summary

- Equivalence relations, classes, and partitions.
  - Every equivalence class is a partition.
  - Every partition is an equivalence class.
- Modular arithmetic and number domains.
  - Partitioning of basic domain by equivalence relation.
  - Computation with representative.
  - Because of congruence properties, choice of representative does not matter.