Math1510 - Discrete Mathematics
Modular arithmetic

University of Newcastle

UoN

Equivalence Classes define Partitions

Theorem

If R is an equivalence relation on a set X, then the set of equivalence classes of R is a partition of X.

Example

The set of all people is partitioned into 366 disjoint sets based on their birthdays.

- If you were born on the 14th of March, then you are in the same equivalence class (under the birthday relation) as Albert Einstein.

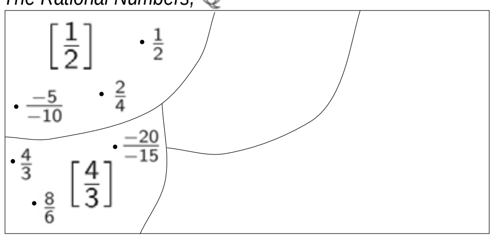
Example (A second Equivalence Classes Example)

- $\left[\frac{1}{2}\right] = \left\{\frac{1}{2}, \frac{2}{4}, \frac{-5}{-10}, \frac{50}{100}, \dots\right\}$
- $\left[\frac{2}{4}\right] = \left[\frac{1}{2}\right]$
- $\left[\frac{4}{3}\right] = \left\{\frac{4}{3}, \frac{8}{6}, \frac{-20}{-15}, \frac{100}{75}, \dots\right\}$

Each of these equivalence classes is the set of all fractions representing the same given rational number. We write $\frac{a}{b} = \frac{c}{d}$ iff $ad = bc$ for $b, d \neq 0$.

This relation is a partition on all pairs of integers $\left[\frac{a}{b}\right]$, $b \neq 0$

The Rational Numbers, $\mathbb{Q}$



This relation can be used to *define* $\mathbb{Q}$ in terms of pairs of elements of $\mathbb{Z}$.

Proof of the Partition Theorem

Theorem

If R is an equivalence relation on a set X, then the set of equivalence classes of R is a partition of X.

Proof outline (see p 161 of textbook for details)

- Define notation. Let X be the set and R be the relation, so that the equivalence class of $a \in X$ is:

$$[a] := \{x \in X : xRa\}$$

and the collection of equivalence classes is

$$S := \{[a] : a \in X\}$$

We need to show:

- for each $a \in X$, the equivalence class $[a]$ is non-empty
- the union of all the classes is the whole set, i.e. $\bigcup S = X$
- pairwise disjointness, i.e. if $x \in X$ and $x \in [a] \cap [b]$ then $[a] = [b]$

The converse is also true

Theorem

Given any partition S on a set X, each of the members of S is an equivalence class, under equivalence relation R given by

$$aRb \iff a \text{ and } b \text{ are in the same member of } S$$

Definition ($\mathbb{Z}_m$ and its arithmetic)

Let $m \geq 2$ be an integer and define the relation

$$a\ R\ b \quad \text{iff} \quad a - b = mk \text{ for some } k \in \mathbb{Z}.$$

Define equivalence classes for each $a \in \mathbb{Z}$ by

$$[a] = \{x \in \mathbb{Z} : x\ R\ a\}$$

Define arithmetic operations addition and multiplication as follows:

$$[a] + [b] = \{x + y : x \in [a], y \in [b]\}$$

$$[a][b] = \{xy : x \in [a], y \in [b]\}$$

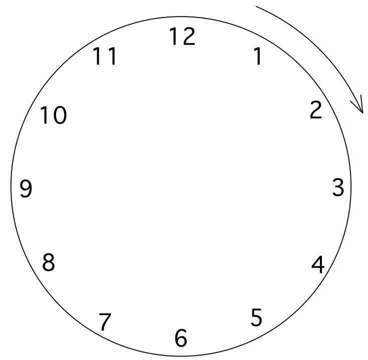
The set of equivalence classes is called $\mathbb{Z}_m$, where m is called the modulus.

$\mathbb{Z}_{12}$, *clock arithmetic:* aRb iff $a - b = 12k$ for $k \in \mathbb{Z}$

$$[0] = \{..., -24, -12, 0, 12, 24, ...\}$$
$$[1] = \{..., -23, -11, 1, 13, 25, ...\}$$
$$[2] = \{..., -22, -10, 2, 14, 26, ...\}$$
$$[3] = \{..., -21, -9, 3, 15, 27, ...\}$$
$$[4] = \{..., -20, -8, 4, 16, 28, ...\}$$
$$[5] = \{..., -19, -7, 5, 17, 29, ...\}$$
$$[6] = \{..., -18, -6, 6, 18, 30, ...\}$$
$$[7] = \{..., -17, -5, 7, 19, 31, ...\}$$
$$[8] = \{..., -16, -4, 8, 20, 32, ...\}$$
$$[9] = \{..., -15, -3, 9, 21, 33, ...\}$$
$$[10] = \{..., -14, -2, 10, 22, 34, ...\}$$
$$[11] = \{..., -13, -1, 11, 23, 35, ...\}$$

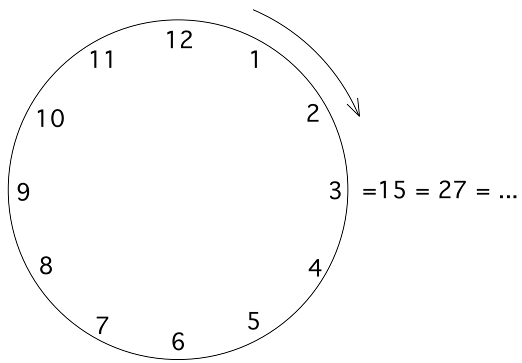
loops back to $[12] = \{..., -12, 0, 12, 24, 36, ...\} = [0]$

$\mathbb{Z}_{12}$, *clock arithmetic:* aRb iff $a - b = 12k$ for $k \in \mathbb{Z}$



- Clock arithmetic wraps around every time you go past 12 o'clock.
- For example, 11 o'clock + 4 hours = 3 o'clock

$\mathbb{Z}_{12}$, *clock arithmetic:* aRb iff $a - b = 12k$ for $k \in \mathbb{Z}$



- Clock arithmetic wraps around every time you go past 12 o'clock.
- For example, 11 o'clock + 4 hours = 3 o'clock

Modular Arithmetic, modulo 12

Clock arithmetic, where we don't bother to write the square brackets, is an example of modular arithmetic.
We write

$$a \equiv b \pmod{12}$$

and say

a is equivalent to b modulo 12

whenever

$$a - b = 12k \text{ for some } k \in \mathbb{Z}$$

Examples of true statements in arithmetic, modulo 12

- $10 + 1 \equiv 11 \pmod{12}$
- $10 + 2 \equiv 12 \pmod{12} \equiv 0 \pmod{12}$ *(ie. wraps around)*
- $10 + 3 \equiv 13 \pmod{12} \equiv 1 \pmod{12}$ "

$\vdots$

Wrapping in modular arithmetic

- To understand the wrapping, look at a smaller modulus.
- $\mathbb{Z}_3$ is defined using equivalence relation aRb if $a - b = 3k$ for $k \in \mathbb{Z}$, giving equivalence classes

$$[0] = \{\ldots -6, -3, 0, 3, 6, \ldots\}$$

$$[1] = \{\ldots -5, -2, 1, 4, 7, \ldots\}$$

$$[2] = \{\ldots -4, -1, 2, 5, 8, \ldots\}$$

$$[3] = \{\ldots -3, 0, 3, 6, 9, \ldots\} = [0] \qquad \textit{(wrapping)}$$

- We choose $[0], [1], [2]$ as standard names for the three classes.

Wrapping in modular arithmetic

- Now recall the definition

$$[a] + [b] = \{x + y : x \in [a], y \in [b]\}$$

$$\begin{aligned}
[0] + [1] &= \{\ldots -6, -3, 0, 3, 6, \ldots\} + \{\ldots -5, -2, 1, 4, 7, \ldots\} \\
&= \\
& \begin{array}{c} \\ \vdots \\ -6 \\ -3 \\ 0 \\ 3 \\ 6 \\ \vdots \end{array}
\begin{array}{c} \ldots\ -5 \quad -2 \quad 1 \quad 4 \quad 7\ \ldots \\ \left\{ \begin{array}{ccccccc} & \vdots & \vdots & \vdots & \vdots & \vdots & \\ \cdots & -11, & -8, & -5, & -2, & 1, & \cdots \\ \cdots & -8, & -5, & -2, & 1, & 4, & \cdots \\ \cdots & -5, & -2, & 1, & 4, & 7, & \cdots \\ \cdots & -2, & 1, & 4, & 7, & 10, & \cdots \\ \cdots & 1, & 4, & 7, & 10, & 13, & \cdots \\ & \vdots & \vdots & \vdots & \vdots & \vdots & \end{array} \right\} \end{array} \\
&= \{\ldots -11, -8, -5, -2, 1, 4, 7, 10, 13, \ldots\} \\
&= [1]
\end{aligned}$$

Addition Table for $\mathbb{Z}_3$

Checking each sum in turn gives:

+	[0]	[1]	[2]
[0]	[0]	[1]	[2]
[1]	[1]	[2]	[0]
[2]	[2]	[0]	[1]

Addition Table for $\mathbb{Z}_3$ and Multiplication Table for $\mathbb{Z}_3$

Checking each sum in turn gives:

+	[0]	[1]	[2]
[0]	[0]	[1]	[2]
[1]	[1]	[2]	[0]
[2]	[2]	[0]	[1]

and products:

·	[0]	[1]	[2]
[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]
[2]	[0]	[2]	[1]

Addition Table for $\mathbb{Z}_3$ and Multiplication Table for $\mathbb{Z}_3$

When the context is clear we do not write the brackets:

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

·	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

Modular arithmetic, modulo m

In $\mathbb{Z}_m$, when we do not write the brackets indicating equivalence classes, we do arithmetic modulo m. We write

$$a \equiv b \pmod{m}$$

and say

a is equivalent to b modulo m

whenever

$$a - b = mk \text{ for some } k \in \mathbb{Z}$$

Which claim is false?

- A $2+3 \equiv 5 \pmod 4$
- B $2+3 \equiv 1 \pmod 4$
- $2+3 \equiv -3 \pmod 4$
- C $2.2 \equiv 0 \pmod 4$ *(the dot means multiplication here)*
- D $2.3 \equiv 1 \pmod 4$

Some comments about Modular Arithmetic

Modular arithmetic has:

- an additive identity, [0],
- a multiplicative identity, [1],
- additive inverses, always, eg in $\mathbb{Z}_3$

$$[1]+[2]=[0]$$

so that [1] is the additive inverse of [2]. *Check all cases!*

- multiplicative inverses, sometimes, e.g. in $\mathbb{Z}_3$,

$$[2][2]=[4]=[1]$$

so that [2] is the multiplicative inverse of itself, but in $\mathbb{Z}_6$ the element [2] has no multiplicative inverse. *What is the important difference between $\mathbb{Z}_3$ and $\mathbb{Z}_6$?*

Check digits

Modulo arithmetic is often exploited in the production of *check digits*, where extra digit(s) are added to a number to verify that it is valid.

Example

ISBN and ISSN use modulo-11 arithmetic to construct and also verify the final digit for the "check digit". To see this, consider the ISBN for Johnsonbaugh: 0-13-135430-2

Our check is that $1d_1 + 2d_2 + 3d_3 + \ldots + 9d_9 \equiv d_{10} \pmod{11}$. If this fails then data did not transfer correctly.

The modulo operator

The operation of finding the remainder on division by n is often written using a *modulo operator*. This is often written mod or %.

Example

In C, C++, Java, and related languages, the statement

```
a = 2016 % 7
```

invokes the calculation $2016 \div 7 = 288$ rem 0 and assigns the value 0 to the variable a.

Rules of Algebra for Modulo arithmetic

If $a \equiv b \pmod{n}$ then

1. $a + c \equiv b + c \pmod{n}$
2. $ac \equiv bc \pmod{n}$
3. $a^2 \equiv b^2 \pmod{n}$

Example

Solve the following equations

- $3x + 1 \equiv 2x + 4 \pmod{6}$
- $4x + 1 \equiv 2x + 4 \pmod{5}$
- $4x + 1 \equiv 2x + 4 \pmod{6}$
- $5x + 1 \equiv 2x + 1 \pmod{7}$

Reciprocals

To solve $2x = 3$ in $\mathbb{R}$, the real number system, we multiply LHS & RHS by $\frac{1}{2}$, the *reciprocal* (a.k.a. *inverse*) of 2.

To see what to do in the corresponding situation for modulo arithmetic, we analyse this more closely:

$$\begin{aligned} 2x &= 3 \\ \implies 2x \times q &= 3 \times q \quad \text{for some suitable } q \\ \implies x \times 2q &= 3q \\ \implies x &= 3q \quad \text{providing } 2q = 1 \end{aligned}$$

This solution relies on finding suitable q such that $2q = 1$, i.e. the *reciprocal of 2*. In $\mathbb{R}$, the suitable number is $\frac{1}{2} = 0{\cdot}5$, and then the solution is $x = 3 \times \frac{1}{2} = \frac{3}{2}$.

We can now look to solve

$$2x \equiv 3 \pmod{5}$$

Use trial and error / observation, to find reciprocal of 2 (this turns out to be 3), then the solution is $x = 3 \times 3 = 9 \equiv 4$ mod 5.

Questions

- Which numbers have reciprocals $\pmod{10}$?
- Which numbers have reciprocals $\pmod{12}$?
- Which numbers have reciprocals $\pmod{7}$?
- Which numbers have reciprocals $\pmod{p}$? For a prime p.
- If a number m has an reciprocal mod n, how do you find it?

Theorem

m has a reciprocal $\pmod{n}$ if and only if the greatest common divisor of m and n is 1.

That is, m has a multiplicative inverse in $\mathbb{Z}_n$ if and only if m and n are coprime/relatively prime/$gcd(m, n) = 1$.

The Euclidean Algorithm

If a number m has a reciprocal $(\mathrm{mod}\ n)$, how do you find it?
The *Euclidean Algorithm*.
This allows you to find the greatest common divisor of m and n, denoted $\gcd(m, n)$, and then s and t such that $sm + tn = \gcd(m, n)$. Once s and t are found, if $\gcd(m, n) = 1$, then $sm \equiv 1 \pmod{n}$ so that s is the reciprocal of m.

Example

Find the gcd(246, 144).

$$\begin{aligned} (246, 144): &\quad 246 = 1 \times 144 + 102 \\ (144, 102): &\quad 144 = 1 \times 102 + 42 \\ (102, 42): &\quad 102 = 2 \times 42 + 18 \\ (42, 18): &\quad 42 = 2 \times 18 + 6 \\ (18, 6): &\quad 18 = 3 \times 6 + 0 \end{aligned}$$

We stop when the remainder is 0 and conclude $\gcd(246, 144) = 6$

Since the gcd is not 1, there is no multiplicative inverse of 144 (mod 246).
If the gcd was one, we could continue and find the inverse!

Example

Find the reciprocal of 7 (mod 18)
Stage 1:

$$\begin{aligned} (18, 7): &\quad 18 = 2 \times 7 + 4 \quad \Rightarrow \quad 4 = 18 - 2 \times 7 \\ (7, 4): &\quad 7 = 1 \times 4 + 3 \quad \Rightarrow \quad 3 = 7 - 1 \times 4 \\ (4, 3): &\quad 4 = 1 \times 3 + 1 \quad \Rightarrow \quad 1 = 4 - 1 \times 3 \\ (3, 1): &\quad 3 = 3 \times 1 + 0 \quad \text{stop, } \gcd(18, 7) = 1 \end{aligned}$$

Conclusion $\gcd(18, 7) = 1$ and so the reciprocal exists

Example

Stage 2:
Work backwards and substitute the equations on the RHS to write 1 as a combination of each a and b.

$$\begin{aligned} (4, 3): &\quad 1 = 4 - 1 \times 3 \\ (7, 4): &\quad 1 = 4 - 1 \times (7 - 1 \times 4) \\ &\quad\ \ = 4 - 1 \times 7 + 1 \times 4 \\ &\quad\ \ = 2 \times 4 - 1 \times 7 \\ (18, 7): &\quad 1 = 2 \times (18 - 2 \times 7) - 1 \times 7 \\ &\quad\ \ = 2 \times 18 - 4 \times 7 - 1 \times 7 \\ &\quad\ \ = 2 \times 18 - 5 \times 7 \end{aligned}$$

Example

Stage 3:
Since $2 \times 18 - 5 \times 7 = 1$, we have $-5 \times 7 \equiv 1 \pmod{18}$.
Thus $-5 \equiv 13$ is the modulo-18 reciprocal of 7.
Checking, $7 \times 13 = 91 \equiv 1 \pmod{18}$

We can do this procedure with different setting out if you prefer:

Example

Find the reciprocal of 7 (mod 18)
Stage 1:
Start with $(a, b) = (m, n)$ and replace (a, b) with $(b, a \,\%\, b)$, and repeat until $b = 1$. Also, for later reference, write each remainder as a subtraction.

$$\begin{array}{rrcll}
(18,7): & 18 \div 7 & = & 2r4 & \Rightarrow \quad \mathbf{4} = \mathbf{18} - 2 \times \mathbf{7} \\
(7,4): & 7 \div 4 & = & 1r3 & \Rightarrow \quad \mathbf{3} = \mathbf{7} - 1 \times \mathbf{4} \\
(4,3): & 4 \div 3 & = & 1r1 & \Rightarrow \quad \mathbf{1} = \mathbf{4} - 1 \times \mathbf{3} \\
(3,1): & 3 \div 1 & = & 3r0 & \text{stop, } \gcd(18,7) = 1
\end{array}$$

Conclusion $\gcd(18, 7) = 1$ so the reciprocal exists

Example

Stage 2:
Work backwards using the equations on the RHS to write 1 as a combination of each a and b:

$$\begin{array}{rcrcrcl}
(4,3) & : & 1 & = & \mathbf{4} - \mathbf{3} & & \\
(7,4) & : & 1 & = & \mathbf{4} - (\mathbf{7} - \mathbf{4}) & = & 2 \times \mathbf{4} - \mathbf{7} \\
(18,7) & : & 1 & = & 2 \times (\mathbf{18} - 2 \times \mathbf{7}) - \mathbf{7} & = & 2 \times \mathbf{18} - 5 \times \mathbf{7}
\end{array}$$

Stage 3:
Since $sm + tn = 2 \times 18 - 5 \times 7 = 1$, we have $-5 \times 7 \equiv 1 \pmod{18}$.
Thus $-5 \equiv 13$ is the modulo-18 reciprocal of 7.
Checking, $7 \times 13 = 91 \equiv 1 \pmod{18}$

Textbook exercises

Exercise section 3.1

- 53-54

Exercise section 5.3

- 1-11 (find the gcd using the Euclidean algorithm)
- 33-39 (extended Euclidean algorithm to find inverses)