Lecture 2

Equivalence class

Let's assume that set S have a notion of equivalence (equivalence relation).

Then the set S can be split into equivalence classes.

Def Elements a and b belong to the same equivalence class if and only if they are equivalent.

$$[a]_R = \{ x \in S : a \sim x \}$$

aRx

$(a, x) \in R$.

Properties

T1. Every two equivalence classes $[a]_R$ and $[b]_R$ are either equal if

$a \sim b$, or disjoint otherwise.

Proof. 1) Let's assume that $a \sim b$ (i.e. $(a, b) \in R$). Now consider any $c \in [a]_R$, i.e. $a \sim c$.

Then we show that also $(b, c) \in R$

$\Rightarrow c \in [b]_R$.

- $(a, b) \in R$ and this relation is symmetric then $(b, a) \in R$.
- R is also transitive relation, then

$$(b, a) \in R, (a, c) \in R \Rightarrow (b, c) \in R$$

$$\Rightarrow c \in [b]_R.$$

Similarly we prove that if $c \in [b]_R$

$\Rightarrow c \in [a]_R$. Thus in this case

$$[a]_R = [b]_R$$

2) Now let's assume that $(a,b) \notin R$. and there exist such $c \in S$ that $c \in [a]_R$ and $c \in [b]_R$. $\Rightarrow$ $(a,c) \in R$ and $(b,c) \in R$.

From the symmetry and transitivity of R we get that $(a,b) \in R$.

This conclusion contradicts to the assumption that $(a,b) \notin R$. ▶

Def. A set of equivalence classes into which the given set S is split by using the equivalence relation R is called a factor set and denoted S|R.

Residue class

Def. We say that $a \in \mathbb{Z}$ is congruent to $b \in \mathbb{Z}$ modulo $m \in \mathbb{N}$ if m divides the $b-a$, i.e. $b-a = km$, $k \in \mathbb{Z}$ and we write

$$a \equiv b \mod m.$$

T. Congruence modulo m is an equivalence relation R on the integers $\mathbb{Z}$ (reflexivity, symmetry, transitivity, give a proof).

The equivalence class $[a]$ is defined as

$$[a] = \{ b : b \equiv a \mod m \} = a + m\mathbb{Z}.$$

Ex. The factor set for $m = 5$

$$\mathbb{Z} \mid R = \{ [0], [1], [2], [3], [4] \}.$$

e.g. $[1] = \{ \dots, -9, -4, 1, 6, 11, \dots \}$

For residue class $[a]_R$ element "a" defines the name of this class, but any other element of this class $b \in [a]_R$ also can be used as a name

If $b \in [a]_R \Rightarrow [a]_R = [b]_R$.

The factor set is also denoted as

$$\mathbb{Z} \mid m\mathbb{Z}$$

(a set of residue ~~sto~~ mod m classes).

T. For congruences $a \equiv b \bmod m$ and $c \equiv d \bmod m$, the following statements are valid (give proofs)

1) $-a \equiv -b \bmod m$.

2) $a + c \equiv b + d \bmod m$

3) $a \cdot c \equiv b \cdot d \bmod m$.

Natural numbers

The natural numbers $n \in \mathbb{N}$ are the numbers $1, 2, 3, \ldots$

The counting numbers are another term for the natural numbers.

Now we give an axiomatic definition of natural numbers $\mathbb{N}$.

$\mathbb{N}$ is defined by elements of any non-empty set, in which a property succesor is defined having the following properties:

1. There exist an element $1 \in \mathbb{N}$ which is not the successor of any element

2. Every element of $\mathbb{N}$ has one and only one successor which is also a natural number.

3. If the successor of x equals the successor of y, then x equals y.

4. The axiom of induction.

If a statement is true for 1, and if the truth of that statement for an element implies its truth for the successor of that number, then the statement is true for every natural number.

It is clear that $\mathbb{N}$ can be constructed by using these ~~exx~~ioms.

1. $1 \in \mathbb{N}$ by A1.
2. $\exists 2 \in \mathbb{N}$ ① → ② A2
3. 2 is a successor only of 1 by A3.

① → ② → ③ → ....

Mathemat inductio method

T. The statement $T(n)$ is true for any $n \in \mathbb{N}$ if:

1. $T(1)$ is true.
2. $\forall m \in \mathbb{N}$ from truth of $T(m) \Rightarrow$ that $T(m')$ is true for the succesor ~~of~~ m' of m.

A modification (stronger)
principle of Mathematical Induction.

T. If

1) $T(1)$ is true

2) $\forall k \in \mathbb{N}$ we have that

$T(1) \wedge T(2) \wedge \dots \wedge T(k) \Rightarrow T(k+1)$ is true, then

$\forall n \in \mathbb{N}$ the statement $T(n)$ is true

The induction can be started also from $m \neq 1$.

Ex. 1. Let $k_0 = 2$, $k_1 = 3$ and we get a sequence

$$k_{n+1} = 3k_n - 2k_{n-1}.$$

$$k_{n+1} = 3k_n - 2k_{n-1}, \quad k_0 = 1, \; k_1 = 3$$

We want to prove that

$$k_n = 2^n + 1.$$

1. Test initial conditions

$$k_0 = 2^0 + 1 = 1 \quad \text{(true)}$$

$$k_1 = 2^1 + 1 = 3 \quad \text{(true)}$$

$$k_{n+1} = 3k_n - 2k_{n-1} =$$

$$= 3\left(2^n + 1\right) - 2\left(2^{n-1} + 1\right)$$

$$= 3 \cdot 2^n - 1 \cdot 2^n + (3 - 2)$$

$$= 2^{n+1} + 1.$$

Euclidean Algorithm for gcd(a,b)

Def. A common divisor of a and b is an integer that divides both a and b.

T. Among all common divisors of two integers $a, b \in \mathbb{Z}$ which are not both zero, there is exactly one greatest (with respect to $\leq$).
It is called the greatest common divisor ($\gcd(a,b)$) of a and b.

Proof. Let $a \neq 0$. All divisors of 'a' are bounded by $|a|$. Therefore among common divisors of a and b there is a unique greatest.

For completeness we set

$$\gcd(0,0) = 0.$$

Examples

1. $\gcd(18, 30) = 6$
2. $\gcd(-14, 21) = 7$
3. $\gcd(100, 35) = 5$.

How to calculate these results?

The euclidean algorithm is based on the following theorem.

T1. 1) If $b = 0$, then $\gcd(a, b) = |a|$

2) If $b \neq 0$, then

$$\gcd(a, b) = \gcd(|b|, a \bmod |b|).$$

Proof.

1. The first result follows from the definition of gcd.

2. If $a, b \in \mathbb{Z}$ and $b > 0$ there are uniquely determined integers q and r such that

$$a = qb + r \quad \text{and} \quad 0 \leq r < b,$$

namely

$$q = \lfloor a/b \rfloor, \quad r = a - bq$$

(These q and r satisfy the assertion!

1) $a = 21$, $b = 14$.

$q = \lfloor 21/14 \rfloor = 1$, $r = 21 - 14 = 7$

2) $a = 14$, $b = 21$.

$q = \lfloor 14/21 \rfloor = 0$, $r = 14 - 0 \cdot 21 = 14$.

3) $a = -21$, $b = 14$.

$q = \lfloor -21/14 \rfloor = -2$, $r = -21 - (-2) \times 14 = 7$.

Let's continue the proof of 2 part of the theorem

$$a = q|b| + a \bmod |b|.$$

Therefore the greatest common divisor of a and b divides the greatest common divisor of $|b|$ and $a \bmod |b|$ and vice versa.

$\gcd(a, b) \leq \gcd(|b|, a \bmod |b|)$

Example

$$\gcd(100, 35) = \gcd(35, 100 \bmod 35)$$

$$= \gcd(35, 30) = \gcd(30, 5)$$

$$= \gcd(5, 0) = 5.$$

Algorithm

```
gcd(a, b) #
    a = abs(a)   # a = |a|
    b = |b|
    while (b != 0)
        r = a % b   # r = a mod b
        a = b
        b = r
    return a
```

T. The euclidean algorithm computes the greatest common divisor of integer numbers a and b.

Proof. We set $r_0 = |a|$, $r_1 = |b|$ and for $k \geq 1$ and $r_k \neq 0$

$$r_{k+1} = r_{k-1} \bmod r_k .$$

This sequence is computed in the while-loop and after the k-th iteration we have

$$a = r_k , \quad b = r_{k+1}$$

It follows from T1 that $\gcd(a, b)$ is not changed.

There is k such $r_k = 0$, since the sequence $(r_k, k \geq 1)$ is strictly decreasing.

The euclidean algorith computes $\gcd(a, b)$ very efficiently.

Let's assume that $\boxed{a > b > 0.}$

Furthermore let

$$q_k = \lfloor r_{k-1} / r_k \rfloor, \quad 1 \le k \le n.$$

Then we have (since q_k is the quotient of r_{k-1} / r_k)

$$r_{k-1} = q_k r_k + r_{k+1}.$$

Example. $a = 100$, $b = 35$

k	0	1	2	3	4
r_k	100	35	30	5	0
q_k		2	1	6	

Lemma. We have that $q_k \geq 1$ for $1 \leq k \leq n-1$ and

$$\boxed{q_n \geq 2.}$$

Proof. Since $r_{k-1} > r_k > r_{k+1}$ it follows that $q_k \geq 1$, $1 \leq k \leq n$.

Suppose $q_n = 1$. Then $r_{n-1} = r_n$ and this is impossible because the sequence $\{r_k\}$ is strictly decreasing. ▷

T2. Let $\theta = (1+\sqrt{5})/2$. Then the number of iterations in the euclidean algorithm is at most (for $a > b > 0$)

$$(\log b)/(\log \theta) + 1.$$

Proof. Let's assume the worst case $\gcd(a, b) = r_n = 1$.

First we prove that

$$r_k \geq \theta^{n-k}, \quad 0 \leq k \leq n. \qquad (*).$$

Then

$$b = r_1 \geq \theta^{n-1}.$$

Taking logarithms we obtain

$$\boxed{n \leq (\log b)/(\log \theta) + 1.}$$

We prove $(*)$ by induction.

$$r_n = 1 = \theta^0.$$

$$r_{n-1} = q_n r_n = q_n \geq 2 > \theta.$$

Let $n-2 \geq k \geq 0$ and assume that the assertion is true for $k' > k$. Then from Lemma we get

$$r_k = q_{k+1} r_{k+1} + r_{k+2} \geq r_{k+1} + r_{k+2}$$

$$\geq \theta^{n-k-1} + \theta^{n-k-2} = \theta^{n-k-1}\left(1 + \frac{1}{\theta}\right) = \theta^{n-k}.$$

▷