Important!

Validity is sufficient

Every property considered can be reduced to validity:

- *Problem*: Is B a **logical consequence** of $A_1, \ldots, A_n$?
  Equivalent problem: Is the formula $A_1 \wedge \cdots \wedge A_n \rightarrow B$ **valid**?
- *Problem*: Are A and B **logically equivalent**?
  Equivalent problem: Is the formula $A \leftrightarrow B$ **valid**?
- *Problem*: Is A **satisfiable**?
  Equivalent problem: Is $\neg A$ **not valid**?
- *Problem*: Is A a **contradiction**?
  Equivalent problem: Is $\neg A$ **valid**?

Conclusion: The tableau method can also be used to determine logical consequence, logical equivalence, satisfiability and contradiction.

总结：1. A multiplicative inverse of a modulo n exist iff gcd(a, n) = 1.
2. The diophantine equation ax + by = c has a solution iff gcd(a, b) divides c.
3. Linear equation modulo ax ≡ b (mod n) has a solution iff g(a, n) divides b.

$p \rightarrow q \equiv \neg p \vee q$

- For existential quantifier: $\exists x(P(x) \wedge \cdots)$
- For universal quantifier: $\forall x(P(x) \rightarrow \cdots)$

Some important logical equivalences:

1.	$\neg\forall xA \equiv \exists x\neg A$	
2.	$\neg\exists xA \equiv \forall x\neg A$	
3.	$\exists xA \equiv \neg\forall x\neg A$	Elimination of $\exists$
4.	$\forall xA \equiv \neg\exists x\neg A$	Elimination of $\forall$
5.	$\forall x\forall yA \equiv \forall y\forall xA$	Swapping of two $\forall$ quantifiers
6.	$\exists x\exists yA \equiv \exists y\exists xA$	Swapping of to $\exists$ quantifiers
7.	$\forall x(A \wedge B) \equiv \forall xA \wedge \forall xB$	Distribution of $\forall$ over $\wedge$
8.	$\exists x(A \vee B) \equiv \exists xA \vee \exists xB$	Distribution of $\exists$ over $\vee$

∀ ∃ introduce new

Subset $2^{\wedge}$

combination

$$C(n,k) = \frac{P(n,k)}{k!} = \frac{n!}{(n-k)!\,k!}$$

$P(n,k)$

Extended Euclidean Algorithm

until $r_k = 0$ return r_{k-1}

Extended Euclidean algorithm

$r_0 \leftarrow |a|$; $r_1 \leftarrow |b|$; $k \leftarrow 1$;
$s_0 \leftarrow 1$; $s_1 \leftarrow 0$;
$t_0 \leftarrow 0$; $t_1 \leftarrow 1$;
$k \leftarrow 2$;
repeat
  $r_k \leftarrow r_{k-2} \bmod r_{k-1}$;
  $q_k \leftarrow \lfloor r_{k-2}/r_{k-1} \rfloor$;
  $s_k \leftarrow s_{k-2} - q_k s_{k-1}$;
  $t_k \leftarrow t_{k-2} - q_k t_{k-1}$;
  $k \leftarrow k + 1$;
until $r_k = 0$;
return (s_{k-1}, t_{k-1})

We have $r_k = as_k + bt_k$ for $k \geq 0$.
Therefore, the last k with $r_k \neq 0$ gives $s = s_k$, $t = t_k$, such that

$$as + bt = \gcd(a,b) = r_k$$

Example: $\gcd(63, 22)$

k	q_k	r_k	s_k	t_k
-1		63	1	0
0		22	0	1
1	2	19	1	-2
2	1	3	-1	3
3	6	1	7	-20
4	3	0		

Therefore:
$\gcd(63, 22) = 1 = 7 \cdot 63 + -20 \cdot 22$

Diophantine Equation

Definition: Diophantine Equation

A linear algebraic equation in 2 variables x, y with $\mathbb{Z}^+$ valued coefficients a, b, c

$$ax + by = c. \qquad (1)$$

is called a *(linear) diophantine equation* (after Diophantos von Alexandria).

The aim is to find integer solutions, i.e. $x,\ y \in \mathbb{Z}^+$.

The equation

$$18x + 30y = 12$$

has another solution $x = 4$ and $y = -2$, giving: $18 \cdot 4 + 30 \cdot (-2) = 72 - 60 = 12$.

Theorem

The diophantine equation $ax + by = c$ has a solution if and only if $\gcd(a, b)$ divides c.

Solving Diophantine Equations

Given the equation $ax + by = c$

1. Check whether $\gcd(a, b) \mid c$. If not: no solution.
2. Compute s, t for $as + bt = \gcd(a, b)$. Multiply by $f = c/\gcd(a, b)$.
3. Then

$$\begin{aligned} a\underbrace{(fs)}_{=x} + b\underbrace{(ft)}_{=y} &= a\frac{c}{\gcd(a,b)}s + b\frac{c}{\gcd(a,b)}t \\ &= \frac{c}{\gcd(a,b)}\left[as + bt\right] \\ &= \frac{c}{\gcd(a,b)}\gcd(a,b) = c \end{aligned}$$

We have to find a way to compute s, t.

For this we use the Extended Euclidean Algorithm.

Solving Diophantine Equations, Example

Example: Solving $3x + 6y = 30$

k	q_k	r_k	s_k	t_k
-1		3	1	0
0		6	0	1
1	0	3	1	0
2	2	0		

① s, t

② gcd

③ $\frac{c}{gcd} s$ $\frac{c}{gcd} t$

So: $\gcd(3, 6) = 3 = 3 \cdot 1 + 6 \cdot 0$ and $f = c/\gcd(a, b) = 30/3 = 10$ and

$$3 \cdot (10 \cdot 1) + 6 \cdot (10 \cdot 0) = 30$$

That is $x = 10$ and $y = 0$ is a solution.

11

Example: Date and Time

- Which weekday is tomorrow? In 4 days? In 70001 days?
- Christmas Eve is on a Thursday this year. And next year?

Here's a little trick when you are doing modulo operations: Say you are calculating x (mod y), you can subtract any multiple of y from x without changing the result. So if you were to calculate 700000003 (mod 7) you know immediately that the answer is 3 because 700000000 is a multiple of 7. No need to divide big numbers.

$\equiv 3 \pmod 7$

Linear equations modulo n

Theorem

Consider $ax \equiv b \pmod{n}$ and set $d = \gcd(a, n)$.

1. If $d \nmid b$, there is no solution.
2. If $d \mid b$ and $d \neq 1$, the equation is equivalent to

$$(a/d)x \equiv b/d \pmod{(n/d)}$$

   which can be solved as in 3.
3. If $d = 1$ the set of solutions for the equation is given by $cb + n\mathbb{Z}$, with $c = a^{-1}$ a multiplicative inverse of $a \pmod{n}$.

Examples

Find the solutions for

1. $6x \equiv 4 \pmod{27}$
2. $6x \equiv 3 \pmod{27}$
3. $8x \equiv 8 \pmod{28}$

1. $\gcd(6, 27) = 3$ and $3 \nmid 4$: No solution.
2. $\gcd(6, 27) = 3$ and $3 \mid 3$. Equivalent equation is:

$$2x \equiv 1 \pmod{9}$$

   $\gcd(2, 9) = 1$ and $c = 2^{-1} = 5$ ($2 \cdot 5 = 10 \equiv 1 \pmod{9}$).
   Solution set is $5 \cdot 1 + 9\mathbb{Z} = \{\ldots, -4, 5, 14, \ldots\}$
3. $\gcd(8, 28) = 4$ and $4 \mid 8$. Equivalent equation is:

$$2x \equiv 2 \pmod{7}$$

   $\gcd(2, 7) = 1$ and $c = 2^{-1} = 4$ ($2 \cdot 4 = 8 \equiv 1 \pmod{7}$).
   Solution set is $4 \cdot 2 + 7\mathbb{Z} = \{\ldots, -6, 1, 8, 15, \ldots\}$

Simultaneous linear equations modulo n

Now consider systems of linear congruences:

$$\begin{aligned} x &\equiv b_1 \pmod{n_1} \\ x &\equiv b_2 \pmod{n_2} \end{aligned} \tag{1}$$

Theorem

If $\gcd(n_1, n_2) > 1$ and $\tilde{x}$ solves (1), then this system of congruences is equivalent to

$$x \equiv \tilde{x} \pmod{m}$$

with $m = \operatorname{lcm}(n_1, n_2)$ and has the solution set $\tilde{x} + m\mathbb{Z}$.

Example

$$\begin{aligned} x &\equiv 2 \pmod{6} \\ x &\equiv 2 \pmod{8} \end{aligned}$$

has one solution $\tilde{x} = 2$. Then all solutions are given by $2 + 24\mathbb{Z}$

The Chinese remainder theorem (CRT)

Theorem (Sunzi $\approx$ 300)

If $\gcd(n_1, n_2) = 1$ the system of congruences

$$\begin{aligned} x &\equiv b_1 \pmod{n_1} \\ x &\equiv b_2 \pmod{n_2} \end{aligned}$$

is equivalent to

$$x \equiv \underbrace{u_1 n_1 b_2 + u_2 n_2 b_1}_{=v} \pmod{n_1 n_2}$$

where $u_1 = n_1^{-1} \pmod{n_2}$ and $u_2 = n_2^{-1} \pmod{n_1}$. The solution set is $v + n_1 n_2 \mathbb{Z}$

Task

Solve

$$x \equiv 4 \pmod 5$$
$$x \equiv 1 \pmod 2$$

$$x \equiv \underbrace{u_1 n_1 b_2 + u_2 n_2 b_1}_{=v} \pmod{n_1 n_2}$$

$u_1 \equiv 5^{-1} \pmod 2 = 1$
$u_2 \equiv 2^{-1} \pmod 5 = 3$
$v = 1 \cdot 5 \cdot 1 + 3 \cdot 2 \cdot 4 = 29$
$\operatorname{lcm}(5, 2) = 10$
Solution set
$29 + 10\mathbb{Z} = \{\ldots, -1, 9, 19, 29, 39, \ldots\}$

The Chinese remainder theorem (CRT)

Theorem (Sunzi $\approx$ 300)

If $\gcd(n_1, n_2) = 1$ the system of congruences

$$x \equiv b_1 \pmod{n_1}$$
$$x \equiv b_2 \pmod{n_2}$$

is equivalent to

$$x \equiv \underbrace{u_1 n_1 b_2 + u_2 n_2 b_1}_{=v} \pmod{n_1 n_2}$$

where $u_1 = n_1^{-1} \pmod{n_2}$ and $u_2 = n_2^{-1} \pmod{n_1}$. The solution set is $v + n_1 n_2 \mathbb{Z}$

$\gcd(21, 50) = 1$

$31 = 21^{-1} \pmod{50}$ $(31 \cdot 21 = 651 \equiv 1 \pmod{50})$

$8 = 50^{-1} \pmod{21}$ $(8 \cdot 50 = 400 \equiv 1 \pmod{21})$

$v = 31 \cdot 21 \cdot 1 + 8 \cdot 50 \cdot 6 = 3015$

$3051 + 1050\mathbb{Z} = \{\ldots, 3051, 2001, 951, -99, \ldots\}$

multiplicative inverse 看不出来怎么办

$50 u_2 - 1 = 21$

gcd(a, n) ↑50 ↖21

k	r_k	q_k	s_k	t_k
0			21	1	0
1			50	0	1
2	0	21	1	0
3	2	8	-2	1
4	2	5	5	-2
5	1	3	-7	3
6	1	2	12	-5
7	1	1	19	8
8	2	0		

u_1 u_2

Calculating the GCD of polynomials

Use Euclid's algorithm!

Same as over $\mathbb{Z}$, simply use polynomial division:

$r_0 \leftarrow p$; $r_1 \leftarrow q$;
repeat
  $r_k \leftarrow r_{k-2} \bmod r_{k-1}$ //remainder of div. r_{k-2} by r_{k-1} ;
until $r_k = 0$;
return r_{k-1};

$r_k = 0$ 返回 r_{k-1}

Example: Determine $\gcd(x^3 - 4x^2 + 2x - 8, x^2 + 2x + 3)$

As shown earlier $r_2 = (x^3 - 4x^2 + 2x - 8) \bmod (x^2 + 2x + 3) = 11x + 10$.

Next $r_3 = r_1 \bmod r_2 = (x^2 + 2x + 3) \bmod (11x + 10) = 243/121$.

Next $r_4 = r_2 \bmod r_3 = (11x + 10) \bmod 243/121 = 0$.

Therefore $\gcd = 243/121$ or (by the non-uniqueness argument) $\gcd = 1$.

$\times \frac{121}{243}$

Application of the polynomial GCD

Definition: Root of polynomials

A number x_0 is a *root* of polynomial $p(x)$ if $p(x_0) = 0$.

Facts

- A polynomial of degree n has at most n roots.
- A polynomial of odd degree has at least one root.
- At a point x where a polynomial p has a local maximum/minimum its derivative p' has a root.

Theorem: Characterisation of common roots of two polynomials

For polynomials p and q and $d = \gcd(p, q)$, we have

$$p(x_0) = q(x_0) = 0 \iff d(x_0) = 0.$$

A the root of GCD are common roots of

these two polynomials

Tableau concepts

We have the same concepts as for tableaux of propositional logic:

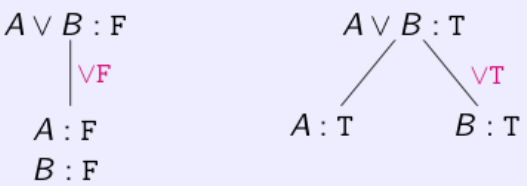
- **Closed branch**: A branch that contains both $A : \mathrm{F}$ and $A : \mathrm{T}$ for a formula A. Closed branches are marked with a cross ($\times$) and there are applied no further rules to them.
- **Open branch**: A branch that is not closed.
- **Saturated branch**: A branch where all rules that **can** be applied **has** been applied. If a branch is both open and saturated it is marked with a circle ($\bigcirc$).

But because of the new tableau rules we have to be more careful about declaring a branch as saturated...

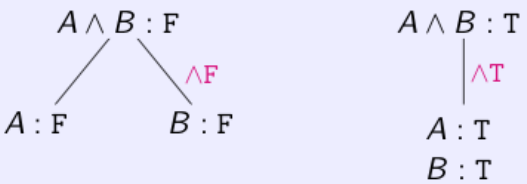
Decomposition rules: negation, disjunction and conjunction

negation

disjunction

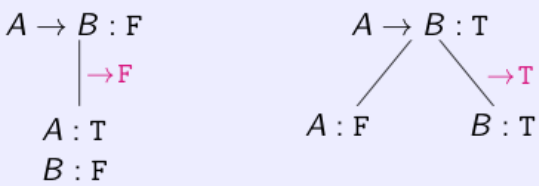


conjunction

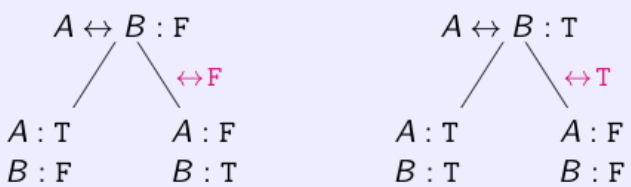


Decomposition rules: implication and biconditional

implication



biconditional



Decomposition rules: universal quantifier

universal quantifer

$$\frac{\forall xA : \mathtt{F}}{A[c/x] : \mathtt{F}}\ \forall\mathtt{F}$$

where c is a **new** constant symbol that does not occur elsewhere on the branch.

$$\frac{\forall xA : \mathtt{T}}{A[t/x] : \mathtt{T}}\ \forall\mathtt{T}$$

where t is a term such that:
1) x is replaceable by t in A.
2) t already occurs earlier on the branch.

Intuition behind $\forall\mathtt{F}$ **rule**. If $\forall xA$ is false, there exists a concrete value of x that makes A false. We **name** this c. We do not yet know which value of x this is, so it is important that c is a **new** constant symbol.

Intuition behind $\forall\mathtt{T}$ **rule**. If $\forall xA$ is true, it is true regardless of the value we let x denote. Therefore, we can insert any other term on the position of x — as long as we do not risk binding variables that are free in t.

Decomposition rules: existential quantifier

existential quantifier

$$\frac{\exists xA : \mathtt{F}}{A[t/x] : \mathtt{F}}\ \exists\mathtt{F}$$

where t is a term such that:
1) x is replaceable by t in A.
2) t already occurs earlier on the branch.

$$\frac{\exists xA : \mathtt{T}}{A[c/x] : \mathtt{T}}\ \exists\mathtt{T}$$

where c is a **new** constant symbol that does not occur elsewhere on the branch.

Intuition behind $\exists\mathtt{F}$ **rule**: As $\forall\mathtt{T}$ rule: (If $\exists xA$ is false, it is false regardless of the value we let x denote. Therefore, we can insert any other term on the position of x — as long as we do not risk binding variables that are free in t.)

Intuition behind $\exists\mathtt{T}$ **rule**: As $\forall\mathtt{F}$ rule.

Notice: Perfect **symmetry** between the $\forall\mathtt{F}$ rule and the $\exists\mathtt{T}$ rule. Likewise between the $\forall\mathtt{T}$ rule and the $\exists\mathtt{F}$ rule.

1

Satisfiability

Definition. A formula is said to be **satisfiable** if it is true in at least one truth assignment.

Equivalent: The formula is true in at least one row of its truth table.

Validity

Definition. A formula is said to be **valid** if it is true in **all** truth assignments.

Equivalent: The formula is true in **all** rows of its truth table.

Example. The formula $p \wedge q \rightarrow p \vee q$ earlier mentioned is **valid** since it is true in all rows of its truth table.

Contradiction

Definition. A formula is called a **contradiction** if it is **false** in **all** truth assignments.

Equivalent: The formula is **false** in **all** rows of its truth table.

Some formulas evaluate to false for every assignment, such formulas are called unsatisfiable formulas or contradictions.

2

Tableau terms

- **Closed branch**: A branch of the talbeau that contains both $A : \mathtt{F}$ and $A : \mathtt{T}$ for a formula A. Closed branches are marked with a cross ($\times$) and no further rules are applied to them.
- **Open branch**: A branch that is not closed.
- **Saturated branch**: A branch where all rules that **can** be applied **have** been applied (which is equivalent to there has been applied a rule on each non-atomic formula of the branch). If a branch is both open and saturated it is marked with a circle ($\bigcirc$).
- **Closed tableau**: A tableau in which all branches are closed.

不能再往下走了

Logical consequence

Definition. A formula B is said to be a **logical consequence** of the formulas $A_1, \ldots, A_n$ if B is always true when all of $A_1, \ldots, A_n$ are true.

More precisely: Every truth assignment that makes all of $A_1, \ldots, A_n$ true, also make B true.

When B is a logical consequence of $A_1, \ldots, A_n$ we write

$$A_1, \ldots, A_n \models B.$$

Logically correct inference

it is also round

Definition. An inference is said to be **logically correct** if its logical form is so that the conclusion is a logical consequence of the premises .

Logically correct inferences are those for which it is **logically impossible** for the premises to be true while the conclusion is false.

The principle of explosion

Consider the following inference rule:

$$\frac{p \wedge \neg p}{q}$$

It seems weird as the conclusion is completely independent from the premise. The rule is however sound as $p \wedge \neg p \models q$.

It is called **the principle of explosion**: From a contradiction, $p \wedge \neg p$, anything can be inferred (an arbitrary proposition q).

Logical equivalence

Definition. Two formulas A and B are said to be **logically equivalent** if they always have the same truth value (has the same truth value in every truth assignment).

When A and B are logically equivalent we write $A \equiv B$.

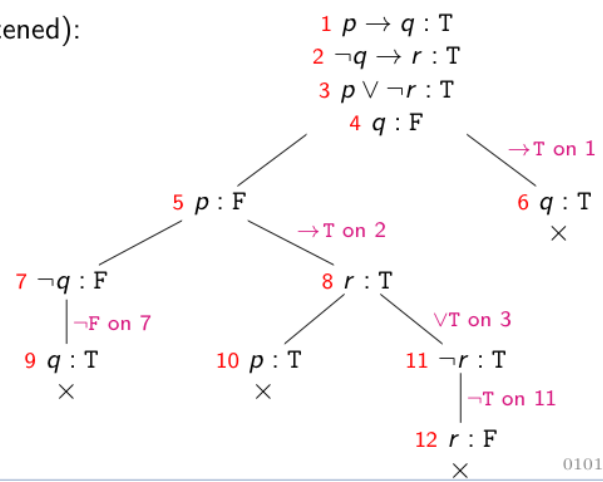
The symbol $\equiv$ is read as 'is logically equivalent to'. As it was the case with $\models$ the symbol is $\equiv$ *not* a logical connective, and $A \equiv B$ is *not* a formula of propositional logic.

Example with logical consequence via tableau.

Show that it holds that $p \to q, \neg q \to r, p \vee \neg r \models q$. It corresponds to showing that the following formula is valid:

$$(p \to q) \wedge (\neg q \to r) \wedge (p \vee \neg r) \to q.$$

Tableau (slightly shortened):



Some important logical equivalences:

$p \vee q \equiv q \vee p$	Commutativity of $\vee$
$p \wedge q \equiv q \wedge p$	Commutativity of $\wedge$
$p \vee (q \vee r) \equiv (p \vee q) \vee r$	Associativity of $\vee$
$p \wedge (q \wedge r) \equiv (p \wedge q) \wedge r$	Associativity of $\wedge$
$p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$	Distributivity of $\wedge$ over $\vee$
$p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$	Distributivity of $\vee$ over $\wedge$
$\neg(p \wedge q) \equiv \neg p \vee \neg q$	De Morgan law
$\neg(p \vee q) \equiv \neg p \wedge \neg q$	De Morgan law
$\neg\neg p \equiv p$	Elimination of $\neg\neg$
$p \leftrightarrow q \equiv (p \rightarrow q) \wedge (q \rightarrow p)$	Elimination of $\leftrightarrow$
$p \rightarrow q \equiv \neg p \vee q$	Elimination of $\rightarrow$

Absorption law
$p \vee (p \wedge q) = p$
$p \wedge (p \vee q) = p$

3

A set can be defined by giving its elements $A = \{4, 2, 9\}$. The order is irrelevant $\{4, 2, 9\}$ is the same as $\{9, 4, 2\}$.

Subsets

Definition. A set A is called a **subset** of a set B if every element of A also is an element of B.

When A is a subset of B we write $A \subseteq B$.

The expression $A \subseteq B$ is called a **set inclusion**.

$A \subset B$, A is a subset of B, but A != B

The set expressions are first translated to formulas of propositional logic:

set expression	**translated to**
$A \cup B$	$A \vee B$
$A \cap B$	$A \wedge B$
$A - B$	$A \wedge \neg B$

Examples. $(A - B) \cup B$ is translated to $(A \wedge \neg B) \vee B$ and $A \cup B$ is translated to $A \vee B$.

Can we also use logical methods to determine set propositions of the form $M \subseteq N$? Yes, translate M and N to formulas of propositional logic **M** and **N** and then determine if $\mathbf{M} \models \mathbf{N}$ holds (or, equivalently, if the formula $M \to N$ is valid).

Set complement

Definition. Let a universal set U be given. **The complement** of a subset $A \subseteq U$ is the set $U - A$. It is usually denoted $\overline{A}$.

Example. Let the universal set be the natural numbers ($U = \mathbb{N}$). The complement of the set of even numbers is then the odd numbers:

$$\overline{E} = O, \text{ where } E = \{x \in \mathbb{N} \mid x \text{ is even}\} \text{ and } O = \{x \in \mathbb{N} \mid x \text{ is odd}\}.$$

Earlier we saw that $A \cup B$ could be translated to $A \vee B$, $A \cap B$ to $A \wedge B$ and $A - B$ to $A \wedge \neg B$. What is the translation of $\overline{A}$ to a formula of propositional logic? It is the formula $\neg A$.

Tuples

Properties of sets:

- Are **solely** characterized by **which** elements they contain.
- **The order** in which we state the elements is therefore irrelevant.
- It is also irrelevant if we **repeat** the same element multiple times.

Example.

$$\{1, 2, 3, 4\} = \{3, 1, 2, 4\} = \{1, 2, 2, 3, 3, 3, 4, 4, 4, 4\}.$$

As an alternative to finite sets we have **tuples**: Expressions of the form $(a_1, \ldots, a_n)$.

The expression $(a_1, \ldots, a_n)$ is a called an n-**tuple** (a **pair** if $n = 2$).

Tuples are ordered, i.e. the order and repetitions are no longer irrelevant:

$$(1, 2, 3, 4) \neq (3, 1, 2, 4) \neq (1, 2, 2, 3, 3, 3, 4, 4, 4, 4).$$

Cross product of two sets

Notice: The cross product gives **all** possible combinations of an element from C with an element from G.

If A has n elements, and B has m elements, how many elements are then in the cross product $A \times B$? There are $n \cdot m$, since we have to take all possible combinations of an element from A with an element from B.

4 Predicate 不可以作为 Predicate和Function的参数
Function可以作为Predicate和Function的参数

Universal quantifier

The sentence "All humans have two legs" is expressed in the following way in predicate logic:

$$\forall x(H(x) \rightarrow T(x)).$$

This is read as:

"**For all** x *it holds that* $H(x)$ *implies* $T(x)$."

As H represents the property of being a human, and T the property of having two legs, it can also be read as:

"**For all** x *it holds that if* x *is a human then* x *has two legs.*"

In other words:

"All humans have two legs."

Existential quantifier

Consider again the proposition "All humans have two legs" with the following formalization:

$$\forall x(H(x) \rightarrow T(x)).$$

If you instead wanted to express "There exists a human who has two legs", one could write:

$$\exists x(H(x) \wedge T(x)).$$

It is read as:

"**There exists** *an* x *such that* $H(x)$ *and* $T(x)$."

As H represents the property of being a human, and T the property of having two legs, it can also be read as:

"**There exists an** x, *such that* x *is a human and* x *has two legs.*"

In other words:

"There exists a human with two legs."

The ingredients of predicate logic

All ingredients of predicate logic:

- **Constant symbols**. Usually denoted by symbols such as $a, b, c, \ldots$.
- **Function symbols**. Usually denoted by symbols such as $f, g, h, \ldots$. A function symbol is n-ary for an $n \geq 1$.
- **Variables**. Usually denoted by symbols such as $x, y, z, \ldots$.
- **Predicate symbol**. usually denoted by symbols such as $P, Q, R, \ldots$. A predicate symbol is n-ary for an $n \geq 1$.
- **Quantifiers**: $\forall$ and $\exists$.
- **Propositional connectives**: $\neg$, $\vee$, $\wedge$, $\rightarrow$, $\leftrightarrow$.

Above we have through examples hinted how formulas are built from these ingredients. It is clarified in the following...

The recursive structure of terms

More precisely:

Definition. The set of **terms** in predicate logic is defined as follows:

1. Every constant symbol is a term.
2. Every variable is a term.
3. If f is an n-ary function symbol and $t_1, \ldots, t_n$ are terms, then $f(t_1, \ldots, t_n)$ is a term.

Naming of interpretations

Often we give an interpretation a name, e.g. $\mathcal{F}$.

Example. Let $\mathcal{F}$ be an **interpretation** wherein H denotes the predicate "is human" and T denotes the predicate "has two legs". It is written in shorthand in the following way:

$$H^{\mathcal{F}} = \text{is human.}$$
$$T^{\mathcal{F}} = \text{has two legs.}$$

The expression $M^{\mathcal{F}}$ is read as: "the interpretation of M in $\mathcal{F}$." So we have introduced the following notation:

Notation. *If P is a* **predicate symbol** *and $\mathcal{F}$ an* **interpretation**, *we denote the interpretation of P in $\mathcal{F}$ by $P^{\mathcal{F}}$.*

3. $\forall x \forall y (L(x,y) \to L(y,x))$
4. $\forall x (\exists y L(x,y) \to \exists z L(z,x))$

Informally one gets rid of the $H(x) \to \ldots$. What do these formulas express in the interpretation $\mathcal{F}$ from the previous slide? 1. All humans love their mother. 2. All humans love themselves. 3. If a human x loves a human y the converse also holds (mutual love). 4. Everyone that loves someone is also loved by someone.

Predicate symbols vs. function symbols

Husk:

- Predicate symbols express predicates (properties).
- Function symbols express functions.

Is $=$ a predicate symbol or a function symbol? Predicate symbol.

And what about $+$? Function symbol.

And $>$? Predicate symbol.

And $\cdot$ (multiplication)? Function symbol.

"Is subset of" ($\subseteq$) Predicate symbol.

"northern neighbour" Function symbol.

5

Restricted quantification

"Everybody knows someone." In the domain of humans:

$$\forall x \exists y \mathit{Knows}(x,y)$$

"All girls know someone." The universal quantifiers must be **restricted** to girls:

$$\forall x (\mathit{Girl}(x) \to \exists y \mathit{Knows}(x,y)).$$

"All girls know a boy." Now also the existential quantifier must be **restricted** (to boys):

$$\forall x (\mathit{Girl}(x) \to \exists y (\mathit{Boy}(y) \wedge \mathit{Knows}(x,y))).$$

Restricted quantification

The above restriction to quantification over respectively boys and girls are special cases of the following general principle:

Restriction of quantification to the elements of the domain that fulfill the property P is done by:

- For existential quantifier: $\exists x(P(x) \wedge \cdots)$
- For universal quantifier: $\forall x(P(x) \rightarrow \cdots)$

Scopes

Definition. Assume that a formula A contains a quantifier $\forall x$ or $\exists x$. By **the scope** of the quantifier we mean the part of the formula that consists of the quantifier and the parenthesis that comes with it.

Example. Consider the following formula:

$$\forall x\big(\neg R(x,x) \wedge \exists y(R(x,y))\big).$$

The scope of the quantifier $\forall x$ is here the entire formula, while the scope $\exists y$ is the blue subformula.

Example. Scopes of each of the 3 quantifiers marked in blue:

$$\underline{\forall x}(x > 5 \rightarrow \forall y(y < 5 \rightarrow (\exists x(x < 3) \wedge y < x)))$$
$$\forall x(x > 5 \rightarrow \underline{\forall y}(y < 5 \rightarrow (\exists x(x < 3) \wedge y < x)))$$
$$\forall x(x > 5 \rightarrow \forall y(y < 5 \rightarrow (\underline{\exists x}(x < 3) \wedge y < x)))$$

Bound and free variables

Definition. An occurrence of a variable x in a formula is said to be **bound**, if it lies within the scope of a quantifier $\exists x$ or $\forall x$. If not it is said to be **free**.

Example. In the formula $\forall y(R(x,y)) \vee y > 0$ there are two bound occurrences of y (marked in re d) and one free occurrence of (marked in blue). What about x? It has one free occurrence.

Example. Consider the following formula:

$$\exists x \forall z(Q(z,y) \vee \neg \forall y(Q(y,z) \rightarrow P(x))).$$

What is the scope of each of the 3 quantifiers? The scope of $\exists x$ is the entire formula. The scope of $\forall z$ is the entire formula except for $\exists x$. The scope of $\forall y$ is the subformula $\forall y(Q(y,z) \rightarrow P(x))$.

Which occurrences of the 3 variables are free, and which are bound? All occurrences of x and z are bound. The first occurrence of y is free the other two are bounded occurrences.

Open and closed formulas

Definition. A formula is said to be **closed** if all variables only have bound occurrences.

A formula is said to be **open** if all variables only have free occurrences (i.e. the formula has no quantifiers).

Examples. The following formula is **open**:

$$x > 2 \wedge x < 5.$$

The following formula is **closed**:

$$\forall x(x > 2 \wedge x < 5).$$

The following formula is **neither open nor closed**:

$$\forall x(x > 2) \wedge x < 5.$$

Substitution

Definition. Let there be a given formula A, a variable x and a term t. We write $A[t/x]$ for the result of replacing all **free** occurrences of x in A with t. We also say that we **substitute** x by t in A.

Example. Consider again the formula $\forall y(R(x, y)) \vee y > 0$. If we denote this formula A we get:

$$A[t/x] = \forall y(R(t, y)) \vee y > 0.$$
$$A[t/y] = \forall y(R(x, y)) \vee t > 0.$$

Why have not all occurrences of y been replaced by t in $A[t/y]$? Because only the free occurrences are to be substituted.

因为这里边，所有的A都已经被bound了

Is $(\forall xA)[t/x]$ always the same as $\forall x(A[t/x])$? No, not if x has a free occurrence in A. In the first formula nothing is changed, while in the other the free occurrences of x in A are replaced by t.

The term "replaceability"

constant variable function

Definition. Let A be a formula, x a variable and t a term. We say that x is **replaceable** by t in A if no variable in t becomes bound by substituting x by t in A.

Equivalent: x is **replaceable** by t in A if the substitution $A[t/x]$ yields no new bound variable occurrences.

Example. y is **not** replaceable by $f(x)$ in the formula $\exists x(x > y)$, as the x in $f(x)$ would become bound if inserted at the position of y. On the other hand y is replaceable by $f(y)$.

Is y replaceable by x in the formula $\forall x(P(y) \vee P(x))$? No, if we insert x at the position of y it will become bound.

Is y replaceable by x in the formula $y = 5 \vee \forall x \forall y(x > y)$? Yes, since it is only the free occurrence of y in the subformula $y = 5$ that is substituted.

Note: If x is replaceable by t you also say that "t is free for x".

Satisfiability and validity

Definition. A closed formula A is called **satisfiable** if it is true in at least one interpretation.

A closed formula A is called **valid** if it is true in every interpretation. We then often write:

$$\models A.$$

Note: Same terms as for propositional logic, except that we replaced 'truth assignment' by 'interpretation'.

Showing validity

Strategy to prove that a formula A holds in **any** interpretation: Let $\mathcal{F}$ denote an **arbitrary** interpretation. Show that A holds in this interpretation. If we succeed, we have shown that A holds for an **arbitrary** interpretation, and thereby in **any** interpretation.

Example. We wish to show the validity of the following formula:

$$\forall x P(x) \to \exists x P(x).$$

Proof. We have to show that the formula is true in **any** interpretation. Therefore let there by given an **arbitrary** interpretation $\mathcal{F}$. To show $\mathcal{F} \models \forall x P(x) \to \exists x P(x)$ we have to show that if $\mathcal{F} \models \forall x P(x)$ then $\mathcal{F} \models \exists x P(x)$.

Thus assume $\mathcal{F} \models \forall x P(x)$. Then $P(x)$ is true regardless of the value of x in the domain of $\mathcal{F}$. As the domain is non-empty there must be at least one value of x such that $P(x)$ is true. Therefore $\exists x P(x)$ must be true as well. Which means that $\mathcal{F} \models \exists x P(x)$ holds, as desired. □

satisfiable ∃ true valid ∀ true

Unsatisfiability and non-validity

∀ false ∃ false

- A closed formula A is **unsatisfiable** if and only if $\neg A$ **valid**. Why? A unsatisfiable $\Leftrightarrow$ A is not true in any interpretation $\Leftrightarrow$ A is false in every interpretation $\Leftrightarrow$ $\neg A$ is true in every interpretation $\Leftrightarrow$ $\neg A$ is valid.
- A closed formula A is **non-valid** if and only if $\neg A$ is satisfiable. Why? Same argument as above.

存在错的

Conclusion:

In order to show that a formula A **is not valid**, it is sufficient to find a **countermodel** of A.

6

SELF STUDY

Logical equivalence: Renaming of variables

Lemma.

- Let A be a closed formula wherein x occurs bounded.
- Let y denote a variable that does not at all occur in A.
- Let B denote the result of replacing all occurrences of x within the scope of a quantifier $\exists x$ or $\forall x$ with y.

It then holds that:

$$A \equiv B.$$

Examples. The following logical equivalences follows from the lemma:

$$\forall x(x > 2) \wedge \exists x(x < 5) \equiv \forall x(x > 2) \wedge \exists y(y < 5).$$
$$\forall x \exists x(x > 2) \equiv \forall x \exists y(y > 2).$$
$$\exists x \exists y(\forall x P(x) \rightarrow Q(x, y)) \equiv \exists x \exists y(\forall z P(z) \rightarrow Q(x, y)).$$

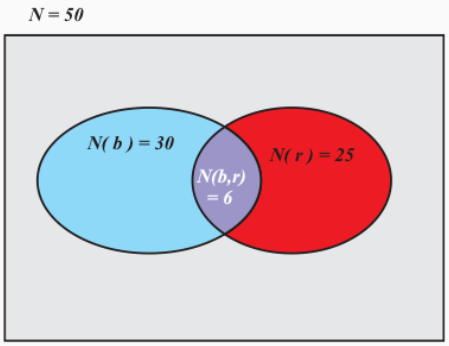
Every closed formula is thus logically equivalent to a **clean formula**: one where the same variable is never bound twice

Inclusion/Exclusion formula

Two properties

Reformulation:

$$\begin{aligned} N(\overline{b},\overline{r}) &= N - N(b) - N(\overline{b},r) \\ &= N - N(b) - (N(r) - N(b,r)) \\ &= \boxed{N - [N(b) + N(r)] + N(b,r)} \end{aligned}$$



Using $N - [N(b) + (N(r)]$ would subtract "area" $N(b,r)$ twice; thus this has to added once to give the correct value of $N(\overline{b},\overline{r})$.

Three properties

Inclusion/exclusion formula

$$\begin{aligned} N(\overline{c}_1,\overline{c}_2,\overline{c}_3) = \quad & N \\ & -[N(c_1) + N(c_2) + N(c_3)] \\ & +[N(c_1,c_2) + N(c_1,c_3) + N(c_2,c_3)] \\ & -N(c_1,c_2,c_3) \end{aligned}$$

Four properties

$$\begin{aligned} & N(\overline{c}_1,\overline{c}_2,\overline{c}_3,\overline{c}_4) = \\ & N & \binom{4}{0} \\ - \quad & [N(c_1) + N(c_2) + N(c_3) + N(c_4)] & \binom{4}{1} \\ + \quad & [N(c_1,c_2) + N(c_1,c_3) + N(c_1,c_4) + N(c_2,c_3) + N(c_2,c_4) + N(c_3,c_4)] & \binom{4}{2} \\ - \quad & [N(c_1,c_2,c_3) + N(c_1,c_2,c_4) + N(c_1,c_3,c_4) + N(c_2,c_3,c_4)] & \binom{4}{3} \\ + \quad & N(c_1,c_2,c_3,c_4) & \binom{4}{4} \end{aligned}$$

Permutations

Permutations are maybe the most important concept in combinatorics.

Definition

Given n distinguishable objects (numbers) $a_1, \ldots, a_n$, a *permutation* is an arrangement of these objects in a linear order.

Example

Let `A,B,C,D` be the objects.

Then
`A,B,C,D`
`C,D,A,B`
`C,B,A,D`
are permutations.

Summary: $n!$ is the number of ways in which n objects can be arranged in a row.

Permutations of lesser size (k-permutations)

The general result

Theorem

Given n distinguishable objects, let $1 \leq k \leq n$. The number of permutations of size k for the n objects is $n \cdot (n-1) \cdots (n-k+1)$.

Notation: We define

$$P(n,k) := n \cdot (n-1) \cdots (n-k+1)$$

Fact:

$$P(n,k) = \frac{n \cdot (n-1) \cdots (n-k+1) \cdot (n-k) \cdots 2 \cdot 1}{(n-k) \cdots 2 \cdot 1} = \frac{n!}{(n-k)!}$$

Identical Objects

The general result.

Theorem

Let n objects be given.

Let there be n_1 indistinguishable objects of Type 1,
n_2 indistinguishable objects of Type 2,
...,
n_r indistinguishable objects of Type r.
Let $n_1 + n_2 + \cdots + n_r = n$.
Then the number of distinguishable linear arrangements of the n objects is

$$\frac{n!}{n_1!\, n_2! \cdots n_r!}$$

Combination

Given n distinguishable objects, a *combination* of size k is a selection of k of the objects without reference to order.

Theorem

Given n distinguishable objects, and $0 \leq k \leq n$. The number $C(n,k)$ of combinations of size k of the n objects is

$$C(n,k) = \frac{P(n,k)}{k!} = \frac{n!}{(n-k)!\, k!}$$

For the proof see the notes.

Notation: $C(n,k)$ is called the binomial coefficient of n and k and is often written as

$$C(n,k) = \binom{n}{k}$$

The symbol $\binom{n}{k}$ is pronounced "n choose k".

Theorem

Let A be a set of n elements and k an integer, $0 \leq k \leq n$. The number of subset $B \subseteq A$ with $|B| = k$ is given by $\binom{n}{k}$.

The Binomial Theorem

Binomial coefficients appear in the expansion of the binomial formula $(x+y)^n$

Example

$$(x+y)^2 = x^2 + 2xy + y^2 = \binom{2}{0}y^2 + \binom{2}{1}xy + \binom{2}{2}x^2$$

$$(x+y)^4 = y^4 + 4xy^3 + 6x^2y^2 + 4x^3y + x^4$$

$$= \binom{4}{0}x^0y^4 + \binom{4}{1}x^1y^3 + \binom{4}{2}x^2y^2 + \binom{4}{3}x^3y^1 + \binom{4}{4}x^4y^0$$

Binomial Theorem

$$(x+y)^n = \binom{n}{0}x^0y^n + \binom{n}{1}x^1y^{n-1} + \ldots + \binom{n}{n}x^ny^0 = \sum_{k=0}^{n}\binom{n}{k}x^ky^{n-k}$$

Identities of Binomial Coefficients

Theorem

For $n, k, m \in \mathbb{N}$ the following identities hold:

$$\sum_{k=0}^{n}\binom{n}{k} = 2^n \tag{5}$$

$$\binom{n}{k} = \binom{n}{n-k} \tag{6}$$

$$\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1} \tag{7}$$

$$\binom{n+m}{k} = \sum_{i=0}^{k}\binom{n}{i}\binom{m}{k-i} \tag{8}$$

8 Well-definedness of recursive definitions

Definition

A recursive definition is *well-defined* if

1. it contains one or more base cases without self-reference; and
2. all other cases can be reduced to the bases cases by using the recursion.

$$f(n) = \begin{cases} 1, & \text{if } n = 0 \\ 2 \cdot f(n/2) & \text{if } n \geq 1 \end{cases}$$

Not well-defined

$$f(n) = \begin{cases} 1, & \text{if } n = 0 \\ 2 \cdot f(n/2) & \text{if } n \geq 1 \end{cases}$$

Recursively defined

Number of k-permutations of n

$$P(n,k) = \begin{cases} 0, & \text{if } k > n \\ 1, & \text{if } k = 0 \\ n \cdot P(n-1, k-1), & \text{if } n \geq k \geq 0 \end{cases}$$

9.

Mathematical Induction

A proof by induction can be carried through if the proposition P depends on natural numbers n.

Mathematical Induction (weak form)

The components of a proof by induction:

Basis step of the induction The proposition $P(n_0)$ holds for $n_0 \in \mathbb{N}$ (often 0 or 1).

Inductive step Show for all $n \geq n_0$ that the following holds: $P(n) \implies P(n+1)$.

Then the induction principle gives that $P(n)$ is true for all natural numbers $n \geq n_0$. The prerequisite $P(n)$ of the implication is called the *Induction hypothesis* or *assumption*.

Mathematical Induction (strong form)

Mathematical Induction (strong form)

Let $P(n)$ be a statement about the natural numbers. If it is true that

1. $P(n_0)$ for a $n_0 \in \mathbb{N}$ and
2. for all $n \geq n_0$ $\quad (\forall k \in \{n_0, n_0+1, \ldots, n\} P(k)) \quad \Rightarrow P(n+1)$

then it must be true that $P(n)$ for all $n \geq n_0$.

Informally: Using that P holds for all lesser numbers, we can conclude that P holds for $n+1$.

The difference to the weak form is, that P holds for **all** numbers from n_0 to n.

$| 0$

Definition: Divisibility of Integers

An integer $d \in \mathbb{Z}$ is called a *divisor* of $n \in \mathbb{Z}$ if there exists a $q \in \mathbb{Z}$ such that

$$n = qd.$$

If d is a divisor in n, it is said that n is a *multiple* of d. We write this as $d \mid n$.

d divides b

Notation:

We write $a\mathbb{Z} = \{ax \mid x \in \mathbb{Z}\}$ for the set of all multiples of a.

Example

$5\mathbb{Z} = \{0, 5, -5, 10, -10, \ldots\}$

Let $a, b, c \in \mathbb{Z}$.

1. $a \mid b \implies ac \mid bc$, for all $c \in \mathbb{Z}$.
2. $(a \mid b) \wedge (a \mid c) \implies a \mid (x \cdot b + y \cdot c)$ for all $x, y \in \mathbb{Z}$.
3. $(a \mid b) \wedge (b \neq 0) \implies |a| \leq |b|$.
4. $(a \mid b) \wedge (b \mid a) \implies |a| = |b|$.

Some proofs are exercises.

Definition: Floor

$\lfloor 4.99 \rfloor = 4$
$\lfloor 5.0 \rfloor = 5$

$$\lfloor x \rfloor = \max\{a \in \mathbb{Z} \mid z \leq x\}$$

Division with remainder

Theorem

Let $n, m \in \mathbb{Z}$ and $m \neq 0$. Then there exist two unambiguous integers $q, r \in \mathbb{Z}$ which fulfill

$$n = qm + r, \text{ and } 0 \leq r < |m|.$$

The integers q and r are called respectively the *quotient* and the *remainder* of the division of n by m.

Example

For a, b find q, r such that $a = qb + r$ and $0 \leq r < |b|$.

- $a = 30, b = 4$ yields $q = 7$, $r = 2$, as $7 \cdot 4 + 2 = 30$.
- $a = -50, b = 8$ yields $q = -7$, $r = 6$, as $-7 \cdot 8 + 6 = -50$.

Modulus Notation

Definition

Let n be a positive integer and $a, b \in \mathbb{Z}$. One says that a and b are *congruent* modulo n if $n \mid (a - b)$ and it is written as

/modzolo/

$$a \equiv b \pmod{n}.$$

The statement $a \equiv b \pmod{n}$ is called a *congruence*, and n is called the *modulus* in this context.

Sometimes modulus is interpreted as an operation, i.e.,

$$r = b \bmod n$$

means that r is the remainder of the division of b by n.

Usually r is the smallest *positive* number with this property.

Greatest Common Divisor

Fact

It holds that $\gcd(n, m) > 0$ for all $n, m \neq 0$. WHY?

gcd(0, 0) = 0

Facts about the GCD

Definition

For $a, b \in \mathbb{Z}$, we set

$$a\mathbb{Z} + b\mathbb{Z} = \{na + mb \mid \ n, m \in \mathbb{Z}\}.$$

Theorem

Let $a, b \in \mathbb{Z}$.

a) Then there exists an unambiguous $d \in \mathbb{N}$ such that $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$. Actually, $d = \gcd(a, b)$.

b) There exist $s, t \in \mathbb{Z}$ such that $\gcd(a, b) = sa + tb$. (Bézout's identity)

The Euclidean Algorithm

Recursive algorithm

Condition $|a| \geq |b|$;
$a \leftarrow |a|$; $b \leftarrow |b|$;
while $b \neq 0$ do
  $r \leftarrow a \bmod b$;
  $a \leftarrow b$;
  $b \leftarrow r$;
end
return a

Iterative algorithm

$r_0 \leftarrow |a|$; $r_1 \leftarrow |b|$;
$k \leftarrow 2$;
repeat
  $r_k \leftarrow r_{k-2} \bmod r_{k-1}$;
  $k \leftarrow k + 1$;
until $r_k = 0$;
return r_{k-1};

The quotients are implicitly given by $q_k = \lfloor r_{k-2}/r_{k-1} \rfloor$, such that $r_{k-2} = r_{k-1} \cdot q_k + r_{k-2} \bmod r_{k-1}$.

Example:
$\gcd(30, 24)$

k	r_k
-1	30
0	24
1	**6**
2	0

Example:
$\gcd(100, -35)$

k	r_k
-1	100
0	35
1	30
2	**5**
3	0

Extended Euclidean Algorithm

Top

Definition

The set of integers congruent to a modulo n:

$$\{b \in \mathbb{Z} \mid b \equiv a \pmod{n}\} = a + n\mathbb{Z}$$

is called the *residue class* of a mod n.

Example

$$-4 + 3\mathbb{Z} = -1 + 3\mathbb{Z} = 2 + 3\mathbb{Z} = 5 + 3\mathbb{Z}$$
$$= \{\ldots, -7, -4, -1, 2, 5, 8, \ldots\}$$

Often use smallest nonnegative element a to describe $a + n\mathbb{Z}$.

Properties of congruences

$\equiv$ has similar properties as $=$

Theorem

1. $a \equiv a \pmod{n}$
2. If $a \equiv b \pmod{n}$ then $b \equiv a \pmod{n}$.
3. If $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$ then $a \equiv c \pmod{n}$.

Theorem (3)

$a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$ implies that:

1. $-a \equiv -b \pmod{n}$
2. $a + c \equiv b + d \pmod{n}$
3. $ac \equiv bd \pmod{n}$

Division modulo n

Goal: solve congruence equations of the form $ax \equiv b \pmod{n}$. How do we divide b by a modulo n?

Definition

We call an integer c such that

$$ca \equiv 1 \pmod{n}$$

a *multiplicative inverse of a modulo n*, written as $a^{-1} \pmod{n}$.

Division modulo n

Theorem

A multiplicative inverse of a modulo n exist iff (if and only if) $\gcd(a, n) = 1$.

Find inverse with extended Euclidean algorithm

If $\gcd(a, n) = 1$ then one can find s, t such that $sn + ta = 1$.
Then because $sn \equiv 0 \pmod{n}$, we have

$$ta + sn \equiv ta + 0 \equiv ta \equiv 1 \pmod{n},$$

so $t = a^{-1} \pmod{n}$.

$sn + ta \equiv 1 \equiv ca \pmod{n}$

$ta \equiv 1 \pmod{n}$

Multiplicative Inverses

- What is a multiplicative inverse of 5 modulo 7?
  As $\gcd(5, 7) = 1$ it exists. Possible choices for $c = 5^{-1} \pmod{7}$ are 3 ($3 * 5 = 15 \equiv 1 \pmod{7}$) or 10 ($10 * 5 = 50 \equiv 1 \pmod{7}$).
- What is a multiplicative inverse of 27 modulo 42?
  As $\gcd(27, 42) = 3$, no solution exists.
- What is a multiplicative inverses of 8 modulo 5?
  As $\gcd(8, 5) = 1$ it exists. Possible choices for $c = 8^{-1} \pmod{5}$ are 2.

Note the multiplicative inverse is not unique. One often chooses the least non-negative number.

7 | 5x - 1 公式

5 | 8x - 1

Calculator:https://planetcalc.com/3311/

Least common multiple

lcm(a, b) = ab/gcd(a, b)

13

Extracting coefficients

For the polynomial $p(x) = \sum_{k=0}^{n} = a_n x^n + \cdots + a_1 x^1 + a_0$, we define

Definition: k^{th} coefficient

$$[x^k]p(x) = \begin{cases} a_k & k \leq n = \deg(p), \\ 0 & k > n \end{cases}$$

Example

For $p(x) = 2x^4 - 3x^2 + 5x - 17$, we have
$[x^2]p(x) = -3$,
$[x^3]p(x) = 0$,
$[x^6]p(x) = 0$.

Example

For $p(x) = (1 + x + 2x^2) \times (3 + 4x + x^2 + x^3)$, what is $[x^9]p(x)$, $[x^5]p(x)$, $[x^0]p(x)$?

0 1 2 0 1 2 3 0 2 3

Division of polynomials

Theorem

Let a, b be polynomials with $b \neq 0$. There exist *unique* polynomials q, r such that $a = bq + r$ with $\deg(r) < \deg(b)$.

Example

$a = x^3 - 4x^2 + 2x - 8$
$b = x^2 + 2x + 3$

$$\begin{array}{r} x - 6 \\ x^2 + 2x + 3 \overline{)\ x^3 - 4x^2 + 2x - 8} \\ -(x^3 - 2x^2 - 3x) \\ \hline -6x^2 + x - 8 \\ -(-6x^2 + 12x + 18) \\ \hline 11x + 10 \end{array}$$

Divisors and the GCD

Definition

A polynomial d is a *divisor* of p if $p = qd$ for some polynomial q. Just as with integers, we write this as $d \mid p$.

Definition

A *common divisor* of two polynomials p and q of maximal degree is called a *greatest common divisor* of p and q, denoted $\gcd(p, q)$.

Example

$$p = 2x^4 - 4x^3 + 2x - 60$$
$$q = -4x^6 + 4x^5 + 24x^4 - 2x^2 + 2x + 12$$

$$d = \gcd(p, q) = 2x^2 - 2x - 12$$

The GCD is **not** unique, because cd is also a GCD for any number $c \neq 0$. However the coefficients might no longer be integers.

$$p = (2x^2 - 2x - 12) \times (x^2 - x + 5)$$
$$p = (4x^2 - 4x - 24) \times (1/2\,x^2 - x/2 + 5/2)$$