Relace a kongruence modulo

Definice

Binární relace R na množině A je podmnožina $R \subseteq A \times A$. Píšeme $x\,R\,y$ (čteme: x je v relaci R s y) místo $(x, y) \in R$.

Příklad

Ať $A = \{a, b, c\}$. Příklady binárních relací na A:

1. $R = \{(a, b), (c, a)\}$. Platí $a\,R\,b$ a také $c\,R\,a$.
2. $\Delta_A = \{(a, a), (b, b), (c, c)\}$. Platí $x\,\Delta_A\,y$ iff $x = y$. Název: diagonála na A nebo identita na A.
3. $A \times A$ je binární relace na A. Je to "největší" možná binární relace na množině A. Platí $x\,(A \times A)\,y$ iff $x, y \in A$.
4. $\emptyset$ je binární relace na A. Je to "nejmenší" možná binární relace na množině A. Pro žádnou dvojici (x, y) neplatí $x\,\emptyset\,y$.

Definice

Binární relace R na množině A je podmnožina $R \subseteq A \times A$. Píšeme $x\,R\,y$ (čteme: x je v relaci R s y) místo $(x, y) \in R$.

Příklad

Ať $A = \{a, b, c\}$. Příklady binárních relací na A:

1. $R = \{(a, b), (c, a)\}$. Platí $a\,R\,b$ a také $c\,R\,a$.
2. $\Delta_A = \{(a, a), (b, b), (c, c)\}$. Platí $x\,\Delta_A\,y$ iff $x = y$. Název: diagonála na A nebo identita na A.
3. $A \times A$ je binární relace na A. Je to "největší" možná binární relace na množině A. Platí $x\,(A \times A)\,y$ iff $x, y \in A$.
4. $\emptyset$ je binární relace na A. Je to "nejmenší" možná binární relace na množině A. Pro žádnou dvojici (x, y) neplatí $x\,\emptyset\,y$.

Definice

Binární relace R na množině A je podmnožina $R \subseteq A \times A$. Píšeme $x\,R\,y$ (čteme: x je v relaci R s y) místo $(x, y) \in R$.

Příklad

Ať $A = \{a, b, c\}$. Příklady binárních relací na A:

1. $R = \{(a, b), (c, a)\}$. Platí $a\,R\,b$ a také $c\,R\,a$.
2. $\Delta_A = \{(a, a), (b, b), (c, c)\}$. Platí $x\,\Delta_A\,y$ iff $x = y$. Název: diagonála na A nebo identita na A.
3. $A \times A$ je binární relace na A. Je to "největší" možná binární relace na množině A. Platí $x\,(A \times A)\,y$ iff $x, y \in A$.
4. $\emptyset$ je binární relace na A. Je to "nejmenší" možná binární relace na množině A. Pro žádnou dvojici (x, y) neplatí $x\,\emptyset\,y$.

Definice

Binární relace R na množině A je podmnožina $R \subseteq A \times A$. Píšeme $x\,R\,y$ (čteme: x je v relaci R s y) místo $(x, y) \in R$.

Příklad

Ať $A = \{a, b, c\}$. Příklady binárních relací na A:

1. $R = \{(a, b), (c, a)\}$. Platí $a\,R\,b$ a také $c\,R\,a$.
2. $\Delta_A = \{(a, a), (b, b), (c, c)\}$. Platí $x\,\Delta_A\,y$ iff $x = y$. Název: diagonála na A nebo identita na A.
3. $A \times A$ je binární relace na A. Je to "největší" možná binární relace na množině A. Platí $x\,(A \times A)\,y$ iff $x, y \in A$.
4. $\emptyset$ je binární relace na A. Je to "nejmenší" možná binární relace na množině A. Pro žádnou dvojici (x, y) neplatí $x\,\emptyset\,y$.

Definice

Binární relace R na množině A je podmnožina $R \subseteq A \times A$. Píšeme $x\,R\,y$ (čteme: x je v relaci R s y) místo $(x, y) \in R$.

Příklad

Ať $A = \{a, b, c\}$. Příklady binárních relací na A:

1. $R = \{(a, b), (c, a)\}$. Platí $a\,R\,b$ a také $c\,R\,a$.
2. $\Delta_A = \{(a, a), (b, b), (c, c)\}$. Platí $x\,\Delta_A\,y$ iff $x = y$. Název: diagonála na A nebo identita na A.
3. $A \times A$ je binární relace na A. Je to "největší" možná binární relace na množině A. Platí $x\,(A \times A)\,y$ iff $x, y \in A$.
4. $\emptyset$ je binární relace na A. Je to "nejmenší" možná binární relace na množině A. Pro žádnou dvojici (x, y) neplatí $x\,\emptyset\,y$.

Definice

Binární relace R na množině A je podmnožina $R \subseteq A \times A$. Píšeme $x\,R\,y$ (čteme: x je v relaci R s y) místo $(x, y) \in R$.

Příklad

Ať $A = \{a, b, c\}$. Příklady binárních relací na A:

1. $R = \{(a, b), (c, a)\}$. Platí $a\,R\,b$ a také $c\,R\,a$.
2. $\Delta_A = \{(a, a), (b, b), (c, c)\}$. Platí $x\,\Delta_A\,y$ iff $x = y$. Název: diagonála na A nebo identita na A.
3. $A \times A$ je binární relace na A. Je to "největší" možná binární relace na množině A. Platí $x\,(A \times A)\,y$ iff $x, y \in A$.
4. $\emptyset$ je binární relace na A. Je to "nejmenší" možná binární relace na množině A. Pro žádnou dvojici (x, y) neplatí $x\,\emptyset\,y$.

Relaci R budeme chtít chápat dvěma různými způsoby:

1. Jako seznam dvojic (x, y), kdy se x má "slepit" s y. Takovým relacím R se říká relace ekvivalence.
   Relace ekvivalence musí mít speciální vlastnosti.
2. Jako seznam dvojic (x, y), kdy x je "menší nebo rovno" y.
   Takovým relacím R se říká relace uspořádání.
   Relace částečného uspořádání musí mít speciální vlastnosti.

Relaci R budeme chtít chápat dvěma různými způsoby:

1. Jako seznam dvojic (x, y), kdy se x má "slepit" s y. Takovým relacím R se říká relace ekvivalence.
   Relace ekvivalence musí mít speciální vlastnosti.
2. Jako seznam dvojic (x, y), kdy x je "menší nebo rovno" y.
   Takovým relacím R se říká relace uspořádání.
   Relace částečného uspořádání musí mít speciální vlastnosti.

Relaci R budeme chtít chápat dvěma různými způsoby:

1. Jako seznam dvojic (x, y), kdy se x má "slepit" s y. Takovým relacím R se říká relace ekvivalence.
   Relace ekvivalence musí mít speciální vlastnosti.
2. Jako seznam dvojic (x, y), kdy x je "menší nebo rovno" y.
   Takovým relacím R se říká relace uspořádání.
   Relace částečného uspořádání musí mít speciální vlastnosti.

Definice

Řekneme, že binární relace R na množině A je:

1. Reflexivní, když pro všechna $x \in A$ platí: $x\,R\,x$.
2. Symetrická, když pro všechna $x, y \in A$ platí: jestliže $x\,R\,y$, pak $y\,R\,x$.
3. Transitivní, když pro všechna $x, y, z \in A$ platí: jestliže $x\,R\,y$ a současně $y\,R\,z$, pak $x\,R\,z$.
4. Antisymetrická, když pro všechna $x, y \in A$ platí: jestliže $x\,R\,y$ a současně $y\,R\,x$, pak $x = y$.
5. Relace ekvivalence, pokud je reflexivní, symetrická a transitivní současně.
6. Relace uspořádání, pokud je reflexivní, antisymetrická a transitivní současně.

Definice

Řekneme, že binární relace R na množině A je:

1. Reflexivní, když pro všechna $x \in A$ platí: $x\,R\,x$.
2. Symetrická, když pro všechna $x, y \in A$ platí: jestliže $x\,R\,y$, pak $y\,R\,x$.
3. Transitivní, když pro všechna $x, y, z \in A$ platí: jestliže $x\,R\,y$ a současně $y\,R\,z$, pak $x\,R\,z$.
4. Antisymetrická, když pro všechna $x, y \in A$ platí: jestliže $x\,R\,y$ a současně $y\,R\,x$, pak $x = y$.
5. Relace ekvivalence, pokud je reflexivní, symetrická a transitivní současně.
6. Relace uspořádání, pokud je reflexivní, antisymetrická a transitivní současně.

Definice

Řekneme, že binární relace R na množině A je:

1. Reflexivní, když pro všechna $x \in A$ platí: $x\,R\,x$.
2. Symetrická, když pro všechna $x, y \in A$ platí: jestliže $x\,R\,y$, pak $y\,R\,x$.
3. Transitivní, když pro všechna $x, y, z \in A$ platí: jestliže $x\,R\,y$ a současně $y\,R\,z$, pak $x\,R\,z$.
4. Antisymetrická, když pro všechna $x, y \in A$ platí: jestliže $x\,R\,y$ a současně $y\,R\,x$, pak $x = y$.
5. Relace ekvivalence, pokud je reflexivní, symetrická a transitivní současně.
6. Relace uspořádání, pokud je reflexivní, antisymetrická a transitivní současně.

Definice

Řekneme, že binární relace R na množině A je:

1. Reflexivní, když pro všechna $x \in A$ platí: $x\,R\,x$.
2. Symetrická, když pro všechna $x, y \in A$ platí: jestliže $x\,R\,y$, pak $y\,R\,x$.
3. Transitivní, když pro všechna $x, y, z \in A$ platí: jestliže $x\,R\,y$ a současně $y\,R\,z$, pak $x\,R\,z$.
4. Antisymetrická, když pro všechna $x, y \in A$ platí: jestliže $x\,R\,y$ a současně $y\,R\,x$, pak $x = y$.
5. Relace ekvivalence, pokud je reflexivní, symetrická a transitivní současně.
6. Relace uspořádání, pokud je reflexivní, antisymetrická a transitivní současně.

Definice

Řekneme, že binární relace R na množině A je:

1. Reflexivní, když pro všechna $x \in A$ platí: $x\,R\,x$.
2. Symetrická, když pro všechna $x, y \in A$ platí: jestliže $x\,R\,y$, pak $y\,R\,x$.
3. Transitivní, když pro všechna $x, y, z \in A$ platí: jestliže $x\,R\,y$ a současně $y\,R\,z$, pak $x\,R\,z$.
4. Antisymetrická, když pro všechna $x, y \in A$ platí: jestliže $x\,R\,y$ a současně $y\,R\,x$, pak $x = y$.
5. Relace ekvivalence, pokud je reflexivní, symetrická a transitivní současně.
6. Relace uspořádání, pokud je reflexivní, antisymetrická a transitivní současně.

Definice

Řekneme, že binární relace R na množině A je:

1. Reflexivní, když pro všechna $x \in A$ platí: $x\,R\,x$.
2. Symetrická, když pro všechna $x, y \in A$ platí: jestliže $x\,R\,y$, pak $y\,R\,x$.
3. Transitivní, když pro všechna $x, y, z \in A$ platí: jestliže $x\,R\,y$ a současně $y\,R\,z$, pak $x\,R\,z$.
4. Antisymetrická, když pro všechna $x, y \in A$ platí: jestliže $x\,R\,y$ a současně $y\,R\,x$, pak $x = y$.
5. Relace ekvivalence, pokud je reflexivní, symetrická a transitivní současně.
6. Relace uspořádání, pokud je reflexivní, antisymetrická a transitivní současně.

Definice

Řekneme, že binární relace R na množině A je:

1. Reflexivní, když pro všechna $x \in A$ platí: $x\,R\,x$.
2. Symetrická, když pro všechna $x, y \in A$ platí: jestliže $x\,R\,y$, pak $y\,R\,x$.
3. Transitivní, když pro všechna $x, y, z \in A$ platí: jestliže $x\,R\,y$ a současně $y\,R\,z$, pak $x\,R\,z$.
4. Antisymetrická, když pro všechna $x, y \in A$ platí: jestliže $x\,R\,y$ a současně $y\,R\,x$, pak $x = y$.
5. Relace ekvivalence, pokud je reflexivní, symetrická a transitivní současně.
6. Relace uspořádání, pokud je reflexivní, antisymetrická a transitivní současně.

Definice

Ať R a S jsou binární relace na množině A.

1. Opačná relace k relaci R je binární relace značená R^{op} s vlastností $x\ R^{op}\ y$ právě tehdy, když $y\ R\ x$.
2. Složení relací R a S je binární relace značená $R;S$ s vlastností $x\ R;S\ y$ právě tehdy, když existuje $z \in A$ takové, že $x\ R\ z$ a současně $z\ S\ y$. Prvku z říkáme prostředník vztahu $x\ R;S\ y$.

Pozor!

Značení je jiné než ve skriptu

M. Demlová a B. Pondělíček, *Matematická logika*, skriptum FEL, 1997.

Definice

Ať R a S jsou binární relace na množině A.

1. Opačná relace k relaci R je binární relace značená R^{op} s vlastností $x\ R^{op}\ y$ právě tehdy, když $y\ R\ x$.
2. Složení relací R a S je binární relace značená $R;S$ s vlastností $x\ R;S\ y$ právě tehdy, když existuje $z \in A$ takové, že $x\ R\ z$ a současně $z\ S\ y$. Prvku z říkáme prostředník vztahu $x\ R;S\ y$.

Pozor!

Značení je jiné než ve skriptu

M. Demlová a B. Pondělíček, *Matematická logika*, skriptum FEL, 1997.

Definice

Ať R a S jsou binární relace na množině A.

1. Opačná relace k relaci R je binární relace značená R^{op} s vlastností $x\ R^{op}\ y$ právě tehdy, když $y\ R\ x$.
2. Složení relací R a S je binární relace značená $R;S$ s vlastností $x\ R;S\ y$ právě tehdy, když existuje $z \in A$ takové, že $x\ R\ z$ a současně $z\ S\ y$. Prvku z říkáme prostředník vztahu $x\ R;S\ y$.

Pozor!

Značení je jiné než ve skriptu

M. Demlová a B. Pondělíček, *Matematická logika*, skriptum FEL, 1997.

Definice

Ať R a S jsou binární relace na množině A.

1. Opačná relace k relaci R je binární relace značená R^{op} s vlastností $x\ R^{op}\ y$ právě tehdy, když $y\ R\ x$.
2. Složení relací R a S je binární relace značená $R;S$ s vlastností $x\ R;S\ y$ právě tehdy, když existuje $z \in A$ takové, že $x\ R\ z$ a současně $z\ S\ y$. Prvku z říkáme prostředník vztahu $x\ R;S\ y$.

Pozor!

Značení je jiné než ve skriptu

> M. Demlová a B. Pondělíček, *Matematická logika*, skriptum FEL, 1997.

Tvrzení

Ať R je binární relace na množině A. Pak platí:

1. *Relace R je reflexivní iff $\Delta_A \subseteq R$.*
2. *Relace R je symetrická iff $R = R^{op}$.*
3. *Relace R je transitivní iff $R;R \subseteq R$.*
4. *Relace R je antisymetrická iff $R \cap R^{op} \subseteq \Delta_A$.*

Pozor!

Relace R na A je symetrická a antisymetrická současně iff $R \subseteq \Delta_A$.

Z toho, že je relace symetrická tedy neplyne, že je antisymetrická (a naopak).

Tvrzení

Ať R je binární relace na množině A. Pak platí:

1. *Relace R je reflexivní iff $\Delta_A \subseteq R$.*
2. *Relace R je symetrická iff $R = R^{op}$.*
3. *Relace R je transitivní iff $R;R \subseteq R$.*
4. *Relace R je antisymetrická iff $R \cap R^{op} \subseteq \Delta_A$.*

Pozor!

Relace R na A je symetrická a antisymetrická současně iff $R \subseteq \Delta_A$.

Z toho, že je relace symetrická tedy neplyne, že je antisymetrická (a naopak).

Tvrzení

Ať R je binární relace na množině A. Pak platí:

1. *Relace R je reflexivní iff $\Delta_A \subseteq R$.*
2. *Relace R je symetrická iff $R = R^{op}$.*
3. *Relace R je transitivní iff $R;R \subseteq R$.*
4. *Relace R je antisymetrická iff $R \cap R^{op} \subseteq \Delta_A$.*

Pozor!

Relace R na A je symetrická a antisymetrická současně iff $R \subseteq \Delta_A$.

Z toho, že je relace symetrická tedy neplyne, že je antisymetrická (a naopak).

Tvrzení

Ať R je binární relace na množině A. Pak platí:

1. *Relace R je reflexivní iff $\Delta_A \subseteq R$.*
2. *Relace R je symetrická iff $R = R^{op}$.*
3. *Relace R je transitivní iff $R;R \subseteq R$.*
4. *Relace R je antisymetrická iff $R \cap R^{op} \subseteq \Delta_A$.*

Pozor!

Relace R na A je symetrická a antisymetrická současně iff $R \subseteq \Delta_A$.

Z toho, že je relace symetrická tedy neplyne, že je antisymetrická (a naopak).

Tvrzení

Ať R je binární relace na množině A. Pak platí:

1. *Relace R je reflexivní iff $\Delta_A \subseteq R$.*
2. *Relace R je symetrická iff $R = R^{op}$.*
3. *Relace R je transitivní iff $R;R \subseteq R$.*
4. *Relace R je antisymetrická iff $R \cap R^{op} \subseteq \Delta_A$.*

Pozor!

Relace R na A je symetrická a antisymetrická současně iff $R \subseteq \Delta_A$.

Z toho, že je relace symetrická tedy neplyne, že je antisymetrická (a naopak).

Tvrzení

Ať R je binární relace na množině A. Pak platí:

1. *Relace R je reflexivní iff $\Delta_A \subseteq R$.*
2. *Relace R je symetrická iff $R = R^{op}$.*
3. *Relace R je transitivní iff $R;R \subseteq R$.*
4. *Relace R je antisymetrická iff $R \cap R^{op} \subseteq \Delta_A$.*

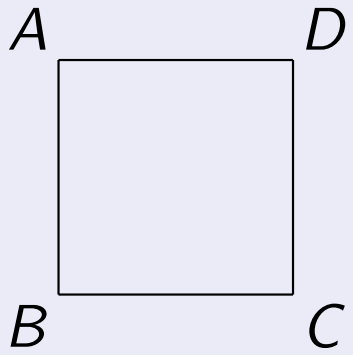
Pozor!

Relace R na A je symetrická a antisymetrická současně iff $R \subseteq \Delta_A$.

Z toho, že je relace symetrická tedy neplyne, že je antisymetrická (a naopak).

Příklad

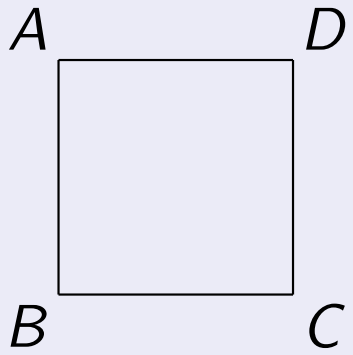
Čtverec $\mathbb{S}$ v rovině:



1. Binární relace R na $\mathbb{S}$: dva body P_1, P_2 čtverce $\mathbb{S}$ jsou v relaci R právě tehdy, když platí buď $P_1 = P_2$ nebo P_1 i P_2 leží na hranici.
   R je relace ekvivalence a dává návod, jak slepit body čtverce: slepte všechny body hranice do jednoho a uvnitř čtverce neslepujte nic.
   Výsledná faktorová množina $\mathbb{S}/R$ (množina $\mathbb{S}$ slepená podle návodu R) je povrch koule, neboli sféra.

Příklad

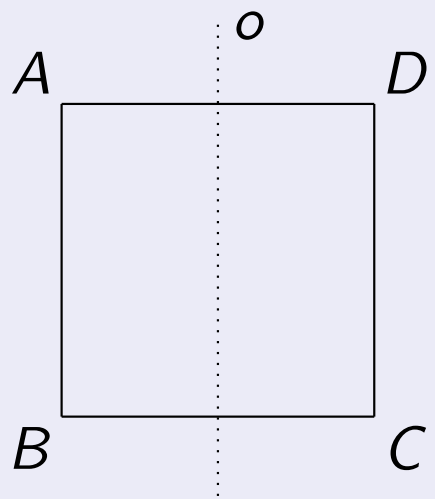
Čtverec $\mathbb{S}$ v rovině:



1. Binární relace R na $\mathbb{S}$: dva body P_1, P_2 čtverce $\mathbb{S}$ jsou v relaci R právě tehdy, když platí buď $P_1 = P_2$ nebo P_1 i P_2 leží na hranici.
   R je relace ekvivalence a dává návod, jak slepit body čtverce: slepte všechny body hranice do jednoho a uvnitř čtverce neslepujte nic.
   Výsledná faktorová množina $\mathbb{S}/R$ (množina $\mathbb{S}$ slepená podle návodu R) je povrch koule, neboli sféra.

Příklad (pokrač.)

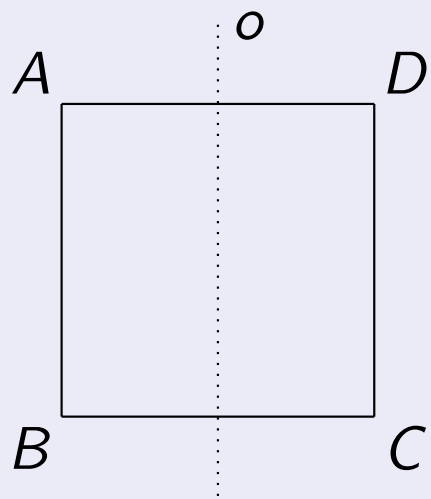
2. Binární relace R na $\mathbb{S}$ taková, že chceme slepit pouze body na úsečce AB s odpovídajícími body na úsečce CD podle symetrie dané osou o



Faktorová množina je válcová plocha.

Příklad (pokrač.)

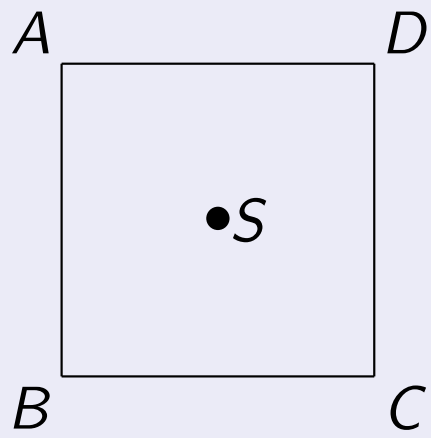
2. Binární relace R na $\mathbb{S}$ taková, že chceme slepit pouze body na úsečce AB s odpovídajícími body na úsečce CD podle symetrie dané osou o



Faktorová množina je válcová plocha.

Příklad (pokrač.)

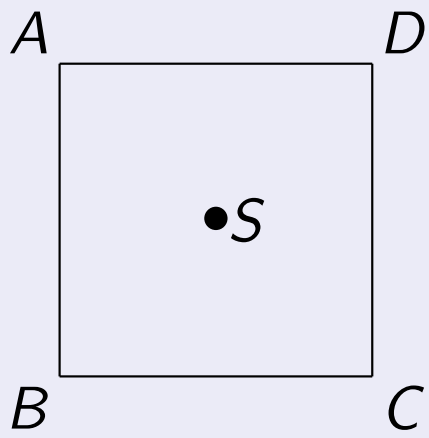
3. Binární relace R na $\mathbb{S}$ taková, že chceme slepit pouze body na úsečce AB s odpovídajícími body na úsečce CD podle symetrie dané bodem S



Faktorová množina je Möbiův list.

Příklad (pokrač.)

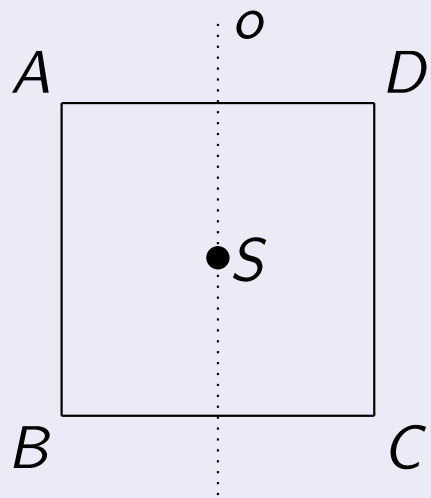
3. Binární relace R na $\mathbb{S}$ taková, že chceme slepit pouze body na úsečce AB s odpovídajícími body na úsečce CD podle symetrie dané bodem S



Faktorová množina je Möbiův list.

Příklad (pokrač.)

4. Binární relace R taková, že chceme slepit pouze body na úsečce AB s odpovídajícími body na úsečce CD podle symetrie dané osou o a body úsečky BC s odpovídajícími body úsečky DA podle symetrie dané bodem S (Möbiův list na válcové ploše):

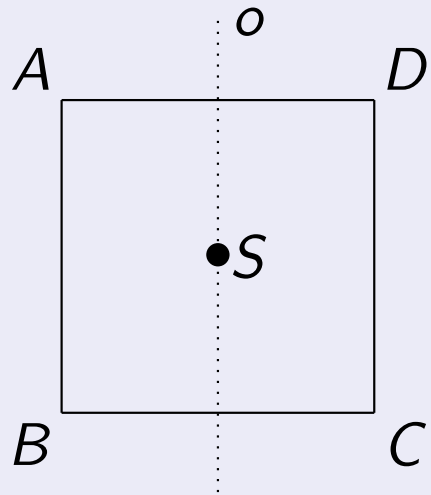


Faktorová množina je Kleinova láhev. [a]

[a] Kleinova láhev není třídimenzionální objekt!

Příklad (pokrač.)

4. Binární relace R taková, že chceme slepit pouze body na úsečce AB s odpovídajícími body na úsečce CD podle symetrie dané osou o a body úsečky BC s odpovídajícími body úsečky DA podle symetrie dané bodem S (Möbiův list na válcové ploše):



Faktorová množina je Kleinova láhev. [a]

[a] Kleinova láhev není třídimensionální objekt!

Shrnuto:

1. Relace ekvivalence R na X je *návod*, jak se mají slepovat prvky množiny X.
2. Po dvojici $\langle X, R \rangle$ se můžeme "procházet", přičemž relace R nám "pokazila zrak".
3. Faktorová množina X/R je množina, kde jsme předepsané dvojice bodů *skutečně slepili*.

Shrnuto:

1. Relace ekvivalence R na X je *návod*, jak se mají slepovat prvky množiny X.
2. Po dvojici $\langle X, R \rangle$ se můžeme "procházet", přičemž relace R nám "pokazila zrak".
3. Faktorová množina X/R je množina, kde jsme předepsané dvojice bodů *skutečně slepili*.

Shrnuto:

1. Relace ekvivalence R na X je *návod*, jak se mají slepovat prvky množiny X.
2. Po dvojici $\langle X, R \rangle$ se můžeme "procházet", přičemž relace R nám "pokazila zrak".
3. Faktorová množina X/R je množina, kde jsme předepsané dvojice bodů *skutečně slepili*.

Shrnuto:

1. Relace ekvivalence R na X je *návod*, jak se mají slepovat prvky množiny X.
2. Po dvojici $\langle X, R \rangle$ se můžeme "procházet", přičemž relace R nám "pokazila zrak".
3. Faktorová množina X/R je množina, kde jsme předepsané dvojice bodů *skutečně slepili*.

Shrnuto:

4. Body (prvky) množiny X/R?
   Slepíme každý bod $x \in X$ se všemi body x', se kterými nám přikazuje relace R bod x slepit:

$$[x]_R = \{x' \in X \mid x\, R\, x'\}$$

Množině $[x]_R$ se říká třída ekvivalence R representovaná prvkem x. Tedy:

$$X/R = \{[x]_R \mid x \in X\}$$

Tvrzení

Zadat ekvivalenci na množině X je totéž jako zadat rozklad množiny X.

Shrnuto:

4. Body (prvky) množiny X/R?
   Slepíme každý bod $x \in X$ se všemi body x', se kterými nám přikazuje relace R bod x slepit:

$$[x]_R = \{x' \in X \mid x\, R\, x'\}$$

   Množině $[x]_R$ se říká třída ekvivalence R representovaná prvkem x. Tedy:

$$X/R = \{[x]_R \mid x \in X\}$$

Tvrzení

Zadat ekvivalenci na množině X je totéž jako zadat rozklad množiny X.

$B(n)$=počet relací ekvivalence na n-prvkové množině

1. Jednoduché: $B(0) = 1$, $B(1) = 1$, $B(2) = 2$.
2. $B(n) = \sum_{k=1}^{n} \binom{n-1}{k-1} \cdot B(n-k)$, $n \geq 1$.

Číslu $B(n)$ říkáme n-té Bellovo číslo.

Rekurence je totéž jako rekursivní algoritmus pro vygenerování všech relací ekvivalence (tj. rozkladů) na množině X:

1. Je-li $X = \emptyset$, pak $\emptyset$ je jediný rozklad.
2. Je-li $X \neq \emptyset$, pak
   1. Vyberte pevné $x \in X$.
   2. Vygenerujte všechny podmnožiny Y množiny $X \setminus \{x\}$.
   3. Pro každou takovou Y: vygenerujte všechny rozklady $X \setminus (\{x\} \cup Y)$ a přidejte $\{x\} \cup Y$.

Pozor!

Krátký vzorec pro Bellova čísla (zatím?) neexistuje. Více o kombinatorických problémech a jejich aplikacích v programování např.

> P. J. Cameron, *Combinatorics: Topics, Techniques, Algorithms*, Cambridge University Press, 1994

nebo

> F. Bergeron, G. Labelle a P. Leroux, *Combinatorial Species and Tree-like Structures*, Cambridge University Press, 2004

Definice

Ať $m \geq 1$ je pevné přirozené číslo. Řekneme, že celá čísla a a b jsou kongruentní modulo m, (značíme $a \equiv b \pmod{m}$), pokud existuje celé číslo k takové, že $a - b = k \cdot m$.

Přeformulování kongruence modulo m

1. Pro $m > 1$: vztah $a \equiv b \pmod{m}$ platí iff a i b mají stejný zbytek po dělení číslem m.
2. Pro $m = 1$: vztah $a \equiv b \pmod{1}$ platí iff a i b jsou celá čísla.

Definice

Ať $m \geq 1$ je pevné přirozené číslo. Řekneme, že celá čísla a a b jsou kongruentní modulo m, (značíme $a \equiv b \pmod{m}$), pokud existuje celé číslo k takové, že $a - b = k \cdot m$.

Přeformulování kongruence modulo m

1. Pro $m > 1$: vztah $a \equiv b \pmod{m}$ platí iff a i b mají stejný zbytek po dělení číslem m.
2. Pro $m = 1$: vztah $a \equiv b \pmod{1}$ platí iff a i b jsou celá čísla.

Tvrzení

Ať $m > 1$ je pevné přirozené číslo. Potom platí:

1. *Kongruence modulo m je relace ekvivalence na množině celých čísel, tj. je reflexivní, symetrická a transitivní.*
2. *Kongruence modulo m respektuje operaci sčítání, tj. pro všechna celá čísla a, b, a', b' platí:*
   jestliže platí $a \equiv b \pmod{m}$ a současně $a' \equiv b' \pmod{m}$, pak platí $a + a' \equiv b + b' \pmod{m}$.
3. *Kongruence modulo m respektuje operaci násobení, tj. pro všechna celá čísla a, b, a', b' platí:*
   jestliže platí $a \equiv b \pmod{m}$ a současně $a' \equiv b' \pmod{m}$, pak platí $a \cdot a' \equiv b \cdot b' \pmod{m}$.

Tvrzení

Ať $m > 1$ je pevné přirozené číslo. Potom platí:

1. *Kongruence modulo m je relace ekvivalence na množině celých čísel, tj. je reflexivní, symetrická a transitivní.*
2. *Kongruence modulo m respektuje operaci sčítání, tj. pro všechna celá čísla a, b, a', b' platí:*
   jestliže platí $a \equiv b \pmod{m}$ a současně $a' \equiv b' \pmod{m}$, pak platí $a + a' \equiv b + b' \pmod{m}$.
3. *Kongruence modulo m respektuje operaci násobení, tj. pro všechna celá čísla a, b, a', b' platí:*
   jestliže platí $a \equiv b \pmod{m}$ a současně $a' \equiv b' \pmod{m}$, pak platí $a \cdot a' \equiv b \cdot b' \pmod{m}$.

Tvrzení

Ať $m > 1$ je pevné přirozené číslo. Potom platí:

1. *Kongruence modulo m je relace ekvivalence na množině celých čísel, tj. je reflexivní, symetrická a transitivní.*
2. *Kongruence modulo m respektuje operaci sčítání, tj. pro všechna celá čísla a, b, a', b' platí:*
   jestliže platí $a \equiv b \pmod{m}$ a současně $a' \equiv b' \pmod{m}$, pak platí $a + a' \equiv b + b' \pmod{m}$.
3. *Kongruence modulo m respektuje operaci násobení, tj. pro všechna celá čísla a, b, a', b' platí:*
   jestliže platí $a \equiv b \pmod{m}$ a současně $a' \equiv b' \pmod{m}$, pak platí $a \cdot a' \equiv b \cdot b' \pmod{m}$.

Tvrzení

Ať $m > 1$ je pevné přirozené číslo. Potom platí:

1. *Kongruence modulo m je relace ekvivalence na množině celých čísel, tj. je reflexivní, symetrická a transitivní.*
2. *Kongruence modulo m respektuje operaci sčítání, tj. pro všechna celá čísla a, b, a', b' platí:*
   jestliže platí $a \equiv b \pmod{m}$ a současně $a' \equiv b' \pmod{m}$, pak platí $a + a' \equiv b + b' \pmod{m}$.
3. *Kongruence modulo m respektuje operaci násobení, tj. pro všechna celá čísla a, b, a', b' platí:*
   jestliže platí $a \equiv b \pmod{m}$ a současně $a' \equiv b' \pmod{m}$, pak platí $a \cdot a' \equiv b \cdot b' \pmod{m}$.

Důsledek

Množinu celých čísel lze "slepit" pomocí kongruence modulo m. Příslušnou faktorovou množinu označíme $\mathbb{Z}_m$.

Lemma

Ať $m > 1$ je pevné přirozené číslo. Potom množina $\mathbb{Z}_m$ má přesně m různých prvků: $\mathbb{Z}_m = \{[0]_m, [1]_m, \ldots, [m-1]_m\}$.
Říkáme jim standardní tvary prvků $\mathbb{Z}_m$.

Příklad

$\mathbb{Z}_6 = \{[0]_6, [1]_6, [2]_6, [3]_6, [4]_5, [5]_6\}$.
Platí například $[2]_6 = [8]_6 = [-4]_6$.
Zjednodušené značení: $2 = 8 = -4$ v $\mathbb{Z}_6$.

Důsledek

Množinu celých čísel lze "slepit" pomocí kongruence modulo m. Příslušnou faktorovou množinu označíme $\mathbb{Z}_m$.

Lemma

Ať $m > 1$ je pevné přirozené číslo. Potom množina $\mathbb{Z}_m$ má přesně m různých prvků: $\mathbb{Z}_m = \{[0]_m, [1]_m, \ldots, [m-1]_m\}$.
Říkáme jim standardní tvary prvků $\mathbb{Z}_m$.

Příklad

$\mathbb{Z}_6 = \{[0]_6, [1]_6, [2]_6, [3]_6, [4]_5, [5]_6\}$.
Platí například $[2]_6 = [8]_6 = [-4]_6$.
Zjednodušené značení: $2 = 8 = -4$ v $\mathbb{Z}_6$.

Důsledek

Množinu celých čísel lze "slepit" pomocí kongruence modulo m. Příslušnou faktorovou množinu označíme $\mathbb{Z}_m$.

Lemma

Ať $m > 1$ je pevné přirozené číslo. Potom množina $\mathbb{Z}_m$ má přesně m různých prvků: $\mathbb{Z}_m = \{[0]_m, [1]_m, \ldots, [m-1]_m\}$.
Říkáme jim standardní tvary prvků $\mathbb{Z}_m$.

Příklad

$\mathbb{Z}_6 = \{[0]_6, [1]_6, [2]_6, [3]_6, [4]_5, [5]_6\}$.
Platí například $[2]_6 = [8]_6 = [-4]_6$.
Zjednodušené značení: $2 = 8 = -4$ v $\mathbb{Z}_6$.

Příklad (pokrač.)

Kongruence modulo 6 respektuje sčítání.

Tabulka pro sčítání v $\mathbb{Z}_6$:

$\oplus_6$	$[0]_6$	$[1]_6$	$[2]_6$	$[3]_6$	$[4]_6$	$[5]_6$
$[0]_6$	$[0]_6$	$[1]_6$	$[2]_6$	$[3]_6$	$[4]_6$	$[5]_6$
$[1]_6$	$[1]_6$	$[2]_6$	$[3]_6$	$[4]_6$	$[5]_6$	$[0]_6$
$[2]_6$	$[2]_6$	$[3]_6$	$[4]_6$	$[5]_6$	$[0]_6$	$[1]_6$
$[3]_6$	$[3]_6$	$[4]_6$	$[5]_6$	$[0]_6$	$[1]_6$	$[2]_6$
$[4]_6$	$[4]_6$	$[5]_6$	$[0]_6$	$[1]_6$	$[2]_6$	$[3]_6$
$[5]_6$	$[5]_6$	$[0]_6$	$[1]_6$	$[2]_6$	$[3]_6$	$[4]_6$

Zjednodušené značení: místo $[3]_6 \oplus [4]_6 = [1]_6$ budeme psát

$$3 + 4 = 1 \text{ v } \mathbb{Z}_6$$

Příklad (pokrač.)

Kongruence modulo 6 respektuje násobení.

Tabulka násobení v $\mathbb{Z}_6$:

$\odot_6$	$[0]_6$	$[1]_6$	$[2]_6$	$[3]_6$	$[4]_6$	$[5]_6$
$[0]_6$	$[0]_6$	$[0]_6$	$[0]_6$	$[0]_6$	$[0]_6$	$[0]_6$
$[1]_6$	$[0]_6$	$[1]_6$	$[2]_6$	$[3]_6$	$[4]_6$	$[5]_6$
$[2]_6$	$[0]_6$	$[2]_6$	$[4]_6$	$[0]_6$	$[2]_6$	$[4]_6$
$[3]_6$	$[0]_6$	$[3]_6$	$[0]_6$	$[3]_6$	$[0]_6$	$[3]_6$
$[4]_6$	$[0]_6$	$[4]_6$	$[2]_6$	$[0]_6$	$[4]_6$	$[2]_6$
$[5]_6$	$[0]_6$	$[5]_6$	$[4]_6$	$[3]_6$	$[2]_6$	$[1]_6$

Zjednodušené značení: místo $[3]_6 \odot [4]_6 = [0]_6$ budeme psát

$$3 \cdot 4 = 0 \text{ v } \mathbb{Z}_6$$