

1. Definujte univerzální systém spojek a dokažte, že (\neg, \wedge) takový systém tvoří.
2. Definujte univerzální systém spojek a dokažte, že (\neg, \vee) takový systém tvoří.

Definice: Je taková množina logických spojek, která každé formuli dožáde přiřadí logicky ekvivalentní formuli, která obsahuje pouze spojky z dané množiny.

Dk: 1) $\{\neg, \wedge\} \Rightarrow$ ukážeme, že pro formule E a F lze vyjádřit $E \vee F$, $E \Rightarrow F$, $E \Leftrightarrow F$ (triv. $E \wedge F$)

$$\begin{aligned} E \vee F &\equiv \neg(\neg E \wedge \neg F) \rightarrow \text{dle De Morganových zákonů} \\ E \Rightarrow F &\equiv \neg E \vee F \equiv \neg(E \wedge \neg F) \rightarrow \text{Zlaté pravidlo + De Morg.} \\ E \Leftrightarrow F &\equiv (E \Rightarrow F) \wedge (F \Rightarrow E) \equiv \neg(E \wedge \neg F) \wedge \neg(F \wedge \neg E) \rightarrow \text{---} \quad \square \end{aligned}$$

2) $\{\neg, \vee\} \Rightarrow$ ukážeme, že pro formule E a F lze vyjádřit $E \wedge F$, $E \Rightarrow F$, $E \Leftrightarrow F$ (triv. $E \vee F$)

$$\begin{aligned} E \wedge F &\equiv \neg(\neg E \vee \neg F) \rightarrow \text{dle De Morganových zákonů} \\ E \Rightarrow F &\equiv \neg E \vee F \rightarrow \text{dle Zlatého pravidla} \\ E \Leftrightarrow F &\equiv (E \Rightarrow F) \wedge (F \Rightarrow E) \equiv (\neg E \vee F) \wedge (\neg F \vee E) \equiv \\ &\equiv \neg(\neg(\neg E \vee F) \vee \neg(\neg F \vee E)) \rightarrow \text{oboje} \quad \square \end{aligned}$$

3. Definujte injektivitu a surjektivitu zobrazení. Dále buďte $f: B \rightarrow C, g: A \rightarrow B$ obě injektivní i surjektivní. Které z těchto vlastností splňuje i $f \circ g$? Své odpovědi dokažte.

Definice: injektivita: Necht' A, B libovolné neprázdné množiny, potom $f: A \rightarrow B$ je injektivní, pokud platí
 $(\forall x, y \in A) (f(x) = f(y) \Rightarrow x = y)$

surjektivita: Necht' A, B libovolné neprázdné množiny,
potom $f: A \rightarrow B$ je surjektivní, pokud platí
 $(\forall y \in B) (\exists x \in A) (f(x) = y)$

Máme $f: B \rightarrow C$, $g: A \rightarrow B$, obě injektivní i surjektivní, chceme
vlastnosti $f \circ g$ ($f \circ g: A \rightarrow C$)

\hookrightarrow Jelikož f i g zároveň prosté i na, potom jsou
bijektivní, tedy každý obraz má právě jeden vzor (1 na 1).
Potom ale i $f \circ g$ nutně bijektivní (prosté i na), neboť
díky f víme, že pro každý prvek $z \in C$ je právě jeden
vzor $z \in B$ a z g víme, že pro každý prvek $z \in B$ je
právě jeden vzor $z \in A$, tedy u $f \circ g$ pro každý prvek
 $z \in C$ existuje právě jeden vzor $z \in A$ (a množina B
slouží jako "prostředník"). □

4. Uveďte, jak ze znalosti booleovské matice relace R na množině $X = \{1, 2, \dots, n\}$ pomocí maticového násobení získat booleovskou matici relace R^2 . Své tvrzení dokažte.

Mějme booleovskou matici M_R relace R s rozměry $n \times n$.

Pro matici složené relace $R \circ R$ (R^2) platí:

$$(M_{R \circ R})_{i,j} = \begin{cases} 1 & \text{pokud } (M_R \cdot M_R)_{i,j} \geq 1 \\ 0 & \text{pokud } (M_R \cdot M_R)_{i,j} = 0 \end{cases}$$

Důk: Z definice maticového násobení víme, že součin $M_R \cdot M_R$
je definován a výsledná matice $M_{R \circ R}$ má rozměry $n \times n$.
Zvolme $i, j \in \{1, 2, \dots, n\}$ libovolně, potom: ($X = \{x_1, \dots, x_n\}$)

$$\begin{aligned} (M_{R \circ R})_{i,j} = 1 &\Leftrightarrow x_i (R \circ R) x_j \Leftrightarrow (\exists x_k \in X) (x_i R x_k \wedge x_k R x_j) \\ &\stackrel{\hookrightarrow (M_{R^2})}{\Leftrightarrow} (\exists k \in \{1, \dots, n\}) (M_{R,i,k} = 1 \wedge M_{R,k,j} = 1) \end{aligned}$$

Ukažme také, kdy $(MR)_{i,j} \geq 1$. To nastane v takovém případě, kdy se v sumě dle definice maticového násobení vyskytne více jedniček, tedy pokud existuje index $k \in \{1, \dots, n\}$, pro který platí $(MR)_{i,k} = 1$ i $(MR)_{k,j} = 1$. To je ovšem podmínka z odvozování výše □

5. Buď R relace ekvivalence na X . Dokažte, že množina $\{[a]_R \mid a \in X\}$ tvoří rozklad množiny X (využijte vlastnosti v definici ekvivalence a definici třídy prvku).

Definice elv.: je taková binární relace R na množině X , která je reflexivní, symetrická, tranzitivní
 $(\Delta_X \subseteq R \subseteq X \times X) \wedge (R^{-1} = R) \wedge (R^2 \subseteq R)$

Definice třídy_prvku: Necht' R relace na množině X . Pro každé $\underline{a} \in X$ definujeme třídu prvku \underline{a} v relaci R jako podmnožinu $[a]_R := \{x \in X \mid x R a\}$

Dk.: Bud' R ekvivalence na X , uvažujme množinu tříd $\{[a]_R \mid a \in X\}$. Z vlastností tříd prvků ekvivalence víme, že $\underline{a} \in [a]_R$ pro každé $\underline{a} \in X$. Tedy všechny třídy nutně neprázdné a navíc splňují podmínku* pokrytí: $(\forall z \in X)(\exists [a]_R)(z \in [a]_R)$. Z vlastností dále víme, že každé dvě třídy jsou disjunktní, tedy je splněna i podmínka** disjunkce.

* pokud $a R b$, pak $[a]_R = [b]_R \Rightarrow$ že symetrie platí $b R a$, stačí tedy ukázat pro libovolné $x \in X$: $x \in [a]_R \Rightarrow x \in [b]_R$ (logicky pak platí i naopak):

$$x \in [a]_R \Rightarrow x R a \xrightarrow{a R b} (x R a \wedge a R b) \xrightarrow{TR} x R b \Rightarrow x \in [b]_R$$

** Necht' $\neg(a R b)$, pro spor předpokládejme $[a]_R \cap [b]_R \neq \emptyset$, tedy $\exists x \in X$, pro které $x R a \wedge x R b$, potom ale $(x R a \wedge x R b) \xrightarrow{SY} (a R x \wedge x R b) \xrightarrow{TR} a R b \rightarrow$ spor a $[a]_R \cap [b]_R = \emptyset$ □

6. Pomocí principu inkluze a exkluze odvoďte vzorec pro derangements t.j. vzorec pro počet permutací n -prvkové množiny, které nezanechávají žádný prvek na svém místě.

Dě: Označme tedy $D_n = n! - |M_1 \cup M_2 \cup \dots \cup M_n|$, kde M_i je množina permutací, které nechávají i -tý prvek na svém místě (ostatní objekty se seřadí jakkoliv). Zároveň $i \in \{1, \dots, n\}$. Potom ale množiny M_i nejsou disjunktivní (např.: identická permutace leží ve všech) \rightarrow proto je potřeba použít PIE.

Zároveň budte $1 \leq i_1 < i_2 < \dots < i_k \leq n$, pak množina $M_{i_1} \cap M_{i_2} \cap \dots \cap M_{i_k}$ obsahuje právě ty permutace, které zachovávají na místě těchto k objektů. Pokud je tedy k objektů zatfixovaných, všech permutací ostatních objektů je $(n-k)!$.

Potom počet permutací, které zanechají něco na svém místě je:

$$\sum_{k=1}^n (-1)^{k-1} \cdot \binom{n}{k} \cdot (n-k)! \quad \begin{cases} \sum_{k=1}^n \Rightarrow \text{kolik objektů} \\ \binom{n}{k} \Rightarrow \text{ktěrych } k \text{ objektů} \\ (n-k)! \Rightarrow \text{kolik je permutací zbytku} \end{cases}$$

\hookrightarrow z definice PIE

$$\begin{aligned} \text{Tedy } D_n &= n! - \sum_{k=1}^n (-1)^{k-1} \cdot \frac{n!}{k!} = \frac{n!}{0!} + \sum_{k=1}^n (-1)^k \cdot \frac{n!}{k!} = \sum_{k=0}^n \frac{(-1)^k \cdot n!}{k!} = \\ &= \underline{\underline{n! \cdot \sum_{k=0}^n \frac{(-1)^k}{k!}}} \end{aligned}$$

□

7. Definujte Stirlingova čísla 1. druhu, napište, jaký rekurentní vztah splňují a tento vztah dokažte.

Definice: Značíme $s(m, n)$ a je to takové číslo, které určuje počet různých permutací libovolné m -prvkové množiny, které mají n cyklů

Rekurentní vztah: $s(m+1, n) = s(m, n-1) + m \cdot s(m, n)$
 \hookrightarrow pro libovolné $m, n \in \mathbb{N}$; $2 \leq n \leq m$

Důkaz: Předpokládejme, že známe počty permutací m -prvkové množiny s libovolným $(1 \leq k \leq m)$ počtem cyklů.
[Uvažme libovolnou $(m+1)$ -prvkovou množinu M . Chceme určit počet jejích permutací s m cykly.] Vybereme si z M libovolný prvek x , pro každou hledanou permutaci π pak platí jedna ze dvou disjunktních možností:

1) x je sám v cyklu délky 1 \Rightarrow permutace zobrazí x na x a dále je jednoznačně určena tím, jak permutuje zbylých m -prvků množiny $M \setminus \{x\}$ ve zbylých $(m-1)$ cyklech $\Rightarrow s(m, m-1)$ permutací

2) x je v cyklu s více prvky \Rightarrow potom uvažme permutaci zbylých m -prvků množiny $M \setminus \{x\}$ s m cykly. Když rozhodneme, kam x vložíme, nestačí pouze vybrat cyklus, kam jej přidáme, ale vybrat přímo jeden z m zbývajících prvků, za kterým v nějakém cyklu bude $\Rightarrow m \cdot s(m, m)$ permutací

Tedy $s(m+1, n) = s(m, n-1) + m \cdot s(m, n)$ □

8. Definujte Stirlingova čísla 2. druhu, napište, jaký rekurentní vztah splňují a tento vztah dokažte.

Definice: Značíme $S(m, n)$ a je to takové číslo, které určuje počet různých rozkladů m -prvkové množiny na n tříd.

Rekurentní vztah: $S(m+1, n) = S(m, n-1) + n \cdot S(m, n)$

$$\hookrightarrow m, n \in \mathbb{N} : 2 \leq n \leq m$$

Dk: Předpokládejme, že známe počty rozkladů m -prvkové množiny do libovolného počtu $(1 \leq k \leq m)$ tříd.

[Uvažme libovolnou $(m+1)$ -prvkovou množinu M . Chceme určit počet rozkladů na n tříd.] Vybereme si z M jeden libovolný prvek x , pro každý hledaný rozklad platí jedna ze dvou disjunktivních možností:

1) x je ve své třídě rozkladu sám \Rightarrow tedy rozklad M jednoznačně určen tím, jak je rozloženo zbylých m prvků množiny $M \setminus \{x\}$ do zbylého počtu $n-1$ tříd $\Rightarrow S(m, n-1)$ rozkladů

2) x je ve víceprvkové třídě \Rightarrow potom uvažujeme rozklad zbylých m prvků $M \setminus \{x\}$ do n tříd. Když rozhodneme, do které z neprázdných n tříd prvek x přidáme, jednoznačně určíme rozklad celé množiny $M \Rightarrow n \cdot S(m, n)$ rozkladů

Tedy $S(m+1) = S(m, n-1) + n \cdot S(m, n)$



9. Na kterých z množin \mathbb{N}_0 , \mathbb{Z} , $\mathbb{N} \setminus \{1\}$ je relace dělitelnosti částečným uspořádáním? Své tvrzení dokažte a v případě, že se jedná o částečné uspořádání, popište maximální, minimální, největší a nejmenší prvky.

Relace dělit. $\Rightarrow (\forall m \in \mathbb{N}_0) (1 \mid m) \text{ a } (m \mid 0)$, to plyne z faktů $1 \cdot m = m$ a $m \cdot 0 = 0$

zda je to částečné uspořádání \Rightarrow ověřit RE, AN, TR

$$X = \mathbb{N}_0, \mathbb{Z}, \mathbb{N} \setminus \{1\}$$

RE) chceme: $(\forall m \in X) (m \mid m)$

\hookrightarrow z definice dělit. $(\forall a, b \in X) (\exists k \in \mathbb{Z}) (a = k \cdot b) \Rightarrow (\forall m \in X) (m = 1 \cdot m)$
 \downarrow
 k

\rightarrow platí pro $\mathbb{N}_0, \mathbb{N} \setminus \{1\}, \mathbb{Z}$

AN) Necht' $t': (\forall a, b \in \mathbb{N} \setminus \{1\} / \mathbb{N}_0) ((a \mid b \wedge b \mid a) \Rightarrow a = b)$

\hookrightarrow Necht' $(\exists k \in \mathbb{Z}) (a \cdot k = b) \wedge (\exists l \in \mathbb{Z}) (b \cdot l = a)$, z toho plyne $a \cdot (k \cdot l) = a$, tedy buď $a = 0$ nebo $k \cdot l = 1$

\hookrightarrow pokud $a = 0$, potom $b = 0 \Rightarrow$ tedy $a = b$ ✓

\hookrightarrow jinak musí pro $k, l \in \mathbb{Z}$ platit $k = l = -1$ (to je ovšem ve sporu s nezáporností a, b), nebo $k = l = 1$ (to vede na $a = b$ ✓)

pro první

\hookrightarrow pro \mathbb{Z} stačí protipříklad, kdy $a = -b$
 \hookrightarrow např. $(3 \mid -3) \wedge (-3 \mid 3) \wedge (3 \neq -3)$

\rightarrow platí pro $\mathbb{N}_0, \mathbb{N} \setminus \{1\}$

TR) chceme: $(\forall a, b, c \in \mathbb{Z} / \mathbb{N}_0 / \mathbb{N} \setminus \{1\}) ((a \mid b \wedge b \mid c) \Rightarrow a \mid c)$

Necht' taková a, b, c splňují $a \mid b \wedge b \mid c$, tedy

$(\exists k \in \mathbb{Z}) (a \cdot k = b) \wedge (\exists l \in \mathbb{Z}) (b \cdot l = c)$

\hookrightarrow z toho přímo plyne $a \cdot (k \cdot l) = c \Rightarrow a \mid c$

\rightarrow platí pro $\mathbb{N}_0, \mathbb{Z}, \mathbb{N} \setminus \{1\}$

• \mathbb{N}_0 : nejmenší (i jediný minimální) je 1 (viz Relace)
 největší (i jediný maximální) je 0 (dělitelnosti)

• $\mathbb{N} \setminus \{1\}$: největší ani maximální prvek/prvky neexistují
 minimální prvky jsou prvočísla, nejmenší není

10. Pro přirozená čísla formulujte větu o jednoznačnosti dělení se zbytkem a tuto větu dokažte.

Věta: Necht' $\underline{a} \in \mathbb{Z}$ a $\underline{d} \in \mathbb{N}$. Pak existují jednoznačně určená čísla $\underline{q}, \underline{r} \in \mathbb{Z}$ taková, že:

$$\underline{a} = \underline{q} \cdot \underline{d} + \underline{r} \quad \text{a} \quad 0 \leq \underline{r} < \underline{d}$$

Číslo \underline{q} nazveme celočíselný podíl, číslo \underline{r} nazveme zbytek po dělení čísla \underline{a} číslem \underline{d} a značíme jej $\underline{r} = \underline{a} \pmod{\underline{d}}$

Dk: Indukcí: uvažujeme nejprve existenci $\underline{q}, \underline{r} \in \mathbb{Z}$ pro všechna $\underline{a} \geq 0$

ZK: Je-li $\underline{a} = 1$, pak $\underline{q} = 0, \underline{r} = 1$ existují ($1 = 0 \cdot \underline{d} + 1$)

IK: Předpokládejme, že pro nějaké $\underline{a} \geq 0$ existují $\underline{q}, \underline{r} \in \mathbb{Z}$ takové, že $\underline{a} = \underline{q} \cdot \underline{d} + \underline{r}$ a $0 \leq \underline{r} < \underline{d}$.

Pak $\underline{a} + 1 = \underline{q} \cdot \underline{d} + (\underline{r} + 1) \wedge 0 \leq (\underline{r} + 1) \leq \underline{d}$. Pokud $(\underline{r} + 1) < \underline{d} \rightarrow$ důkaz hotov

Pokud ovšem $(\underline{r} + 1) = \underline{d}$, pak stačí rovnici upravit na $\underline{a} + 1 = \underline{q} \cdot \underline{d} + \underline{d} = (\underline{q} + 1) \cdot \underline{d} + 0 \quad \checkmark$

Předpokládejme existenci podílu a zbytku pro $\underline{a} < 0 \Rightarrow |\underline{a}| > 0$, tedy existují $\underline{q}, \underline{r} \in \mathbb{Z}$ splňující $|\underline{a}| = -\underline{a} = \underline{q} \cdot \underline{d} + \underline{r}$ a $0 \leq \underline{r} < \underline{d}$. Tedy $\underline{a} = (-\underline{q}) \cdot \underline{d} + (-\underline{r})$

Pokud $\underline{r} = 0$, pak $(-\underline{q})$ hledaný podíl, zbytek 0

V opačném případě :

$$\underline{a} = (-q) \cdot d + (-r) = \underline{(-q-1) \cdot d + (d-r)}$$

kde $0 \leq (d-r) < d$ je zbytek a hledaný podíl $(-q-1)$. Našli jsme tedy dělitele a zbytek pro všechna $\underline{a} \in \mathbb{Z}$

Jednoznačnost : Předpokládejme $q_1, q_2, r_1, r_2 \in \mathbb{Z}$ a $a = q_1 d + r_1 = q_2 d + r_2$ a $0 \leq r_1, r_2 < d$, pak ale $\underline{a = q_1 d + r_1 = q_2 d + r_2} \Rightarrow (q_2 - q_1)d = (r_1 - r_2)$.
Tedy $d \mid (r_1 - r_2)$, současně ale musí platit $0 \leq |r_1 - r_2| < d \Rightarrow r_1 - r_2 = 0 \Rightarrow q_2 - q_1 = 0$ \square

11. Pro $a, b \in \mathbb{N}$ napište, čemu se rovná $\gcd\left(\frac{a}{\gcd(a,b)}, \frac{b}{\gcd(a,b)}\right)$ a své tvrzení dokažte.

Tvrzení : Pro libovolné $a, b \in \mathbb{N}$ platí :

$$\gcd\left(\frac{a}{\gcd(a,b)}, \frac{b}{\gcd(a,b)}\right) = 1$$

Důk : Necht' $\underline{d} = \gcd(a, b)$, chceme ukázat, že $\frac{a}{\underline{d}}$ a $\frac{b}{\underline{d}}$ nemají jiný společný kladný dělitel než 1

Bud' tedy $\underline{e} \in \mathbb{N}$ takové, že $\underline{e} \mid \left(\frac{a}{\underline{d}}\right)$ a $\underline{e} \mid \left(\frac{b}{\underline{d}}\right)$, tedy $(\exists k, l \in \mathbb{Z}) \left(\frac{a}{\underline{d}} = k \cdot \underline{e} \wedge \frac{b}{\underline{d}} = l \cdot \underline{e}\right) \Rightarrow \underline{a} = d \cdot k$ a $\underline{b} = d \cdot l$, tudíž \underline{de} je společný dělitel \underline{a} i \underline{b} .

Ježte \underline{d} je největší společný dělitel \underline{a} a \underline{b} , tedy nutně platí :

$$de \leq d$$

$\Rightarrow \underline{e}$ je rovno 1. To ovšem znamená $\gcd\left(\frac{a}{\underline{d}}, \frac{b}{\underline{d}}\right) = 1$ \square

12. Pro $a, b \in \mathbb{Z}$ napište, jak vypadá řešení diofantické rovnice $ax + by = 0$. Své tvrzení dokažte. Při důkazu můžete využít toho, že pokud $\gcd(a, b) \neq 0$, pak $\gcd\left(\frac{a}{\gcd(a, b)}, \frac{b}{\gcd(a, b)}\right) = 1$ a toho, že $(\gcd(a, b) = 1 \wedge a|bc) \Rightarrow a|c$.

Řešení: Hledáme všechna řešení přidružené homogenní soustavy $ax + by = 0$. Všechna řešení lze zapsat:

$$\left\{ (0, 0) + k \cdot \left(\frac{b}{\gcd(a, b)}, \frac{-a}{\gcd(a, b)} \right), k \in \mathbb{Z} \right\}$$

Důk: Označme $d = \gcd(a, b)$. Vezmeme v potaz triviální řešení $(0, 0)$, které rovnici jistě splňuje (dále (x_0, y_0)).

Chceme popsat obecné řešení (x, y) . Určitě potom platí $ax + by = ax_0 + by_0 \Rightarrow$ tedy $ax - ax_0 = by_0 - by$. Po vydělením d získáme:

$$\frac{a}{d}(x - x_0) = \frac{b}{d}(y_0 - y) *$$

$\Rightarrow \frac{a}{d}$ dělí součin vpravo; $\frac{b}{d}$ dělí součin vlevo
Využijeme toho, že pokud $\gcd(a, b) \neq 0$, pak $\gcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1$.

$$\begin{aligned} \text{Tedy: } \left(\frac{a}{d} \mid \frac{b}{d}(y_0 - y) \wedge \gcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1 \right) &\Rightarrow \frac{a}{d} \mid (y_0 - y) \\ \left(\frac{b}{d} \mid \frac{a}{d}(x - x_0) \wedge \gcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1 \right) &\Rightarrow \frac{b}{d} \mid (x - x_0) \end{aligned}$$

Potom existují $u, v \in \mathbb{Z} \Rightarrow (x - x_0) = u \cdot \frac{b}{d}$ a $(y_0 - y) = v \cdot \frac{a}{d}$

Tedy lze zapsat (dosazení) $\rightarrow \frac{a}{d} \cdot u \cdot \frac{b}{d} = \frac{b}{d} \cdot v \cdot \frac{a}{d} *$

\hookrightarrow z toho plyne $u = v$ (dále přeznačíme $k = u = v$)

Získáme $x = x_0 + \frac{b}{d} \cdot k$ a $y = y_0 - \frac{a}{d} \cdot k$ ($k \in \mathbb{Z}$)

To ovšem znamená, že množina řešení je:

$$\left\{ (x_0, y_0) + k \cdot \left(\frac{b}{\gcd(a, b)}, \frac{-a}{\gcd(a, b)} \right) : k \in \mathbb{Z} \right\}$$



13. Kolik existuje prvočísel? Své tvrzení dokažte.

Tvrzení: Existuje nekonečně mnoho prvočísel.

Dů: Sporem \rightarrow předpokládáme konečně mnoho různých prvočísel $1 < p_1, p_2, p_3, \dots, p_k$ (vesměs prvočísla)

Uvažme potom číslo P takové, že $P = p_1 \cdot p_2 \cdot \dots \cdot p_k + 1$.
Zaučíme $P > 1$, tedy P buď prvočíslo, nebo složené číslo

\hookrightarrow Pokud \underline{P} prvočíslo \Rightarrow spor s " p_1, p_2, \dots, p_k " všechna prvočísla, neboť jsme našli další

\hookrightarrow Pokud \underline{P} složené číslo, pak nutně dělitelné některým z p_1, p_2, \dots, p_k . Označme p_j to, které dělí P .

Tedy $p_j \mid P$, ale i $p_j \mid p_1 \cdot p_2 \cdot \dots \cdot p_k$

\Rightarrow zároveň platí vztah $1 = P - p_1 \cdot p_2 \cdot \dots \cdot p_k$ *

Zde se dá odkázat na tvrzení:

$$(a \mid b \wedge a \mid c) \Leftrightarrow (\forall m, n \in \mathbb{Z})(a \mid (m \cdot b + n \cdot c))$$

\Rightarrow zvolíme tedy $\underline{b} = P$, $\underline{c} = p_1 \cdot p_2 \cdot \dots \cdot p_k$, $\underline{m} = 1$, $\underline{n} = -1$
 $\underline{a} = p_j$, potom ale ze vztahu * plyne, že musí platit $p_j \mid 1 \Rightarrow$ spor s *

\Rightarrow Prvočísel je nekonečně mnoho



14. Formulujte a dokažte Eukleidovo lemma. Při důkazu můžete využít toho, že pokud $\gcd(a, b) \neq 0$, pak $\gcd\left(\frac{a}{\gcd(a, b)}, \frac{b}{\gcd(a, b)}\right) = 1$.

Lemma: Bud' p prvočíslo.

- 1) pokud $p \mid (ab)$, kde $a, b \in \mathbb{N}$ a $p \nmid a$, pak nutně $p \mid b$
- 2) pokud $p \mid (a_1 a_2 \dots a_k)$, kde $a_i (i \in \{1, \dots, k\})$ jsou přirozená čísla, pak existuje $1 \leq j \leq k$ takové, že $p \mid a_j$

Důk: 1) Bezoutova rovnost máme pro dvě nesoudělná čísla (a, p) zaručuje existenci x, y takových, že $px + ay = 1$. Tuto rovnost rozšíříme b , tedy máme $pxb + aby = b$. Zjevně p dělí oba sčítance vlevo ($p \mid ab$) \Rightarrow tedy musí dělit i jejich součet $\Rightarrow p \mid b$.

$$(a \mid b \wedge a \mid c) \Leftrightarrow (\forall m, n \in \mathbb{Z})(a \mid (m \cdot b + n \cdot c))$$

- 2) Indukcí podle $k \in \mathbb{N}$ s využitím bodu 1)
- ZK: $k=1 \Rightarrow$ zjevně platí "pokud $p \mid a_1$, pak $p \mid a_1$ "
- $k=2 \Rightarrow$ plyne z bodu 1)

IK: $k \geq 2$, necht' pro libovolných k přirozených č. platí $(p \mid (a_1 \dots a_k) \Rightarrow (\exists j \in \{1, \dots, k\})(p \mid a_j))$

Uvažujme libovolnou $(k+1)$ -tici přirozených čísel, předpokládejme, že $p \mid (a_1 \dots a_k \cdot a_{(k+1)})$. Vhodně uzavíráme a přeznačíme na:

$$p \mid (\underbrace{a_1}_{a_1} \cdot \underbrace{a_2 \dots a_k \cdot a_{(k+1)}}_b)$$

$\xRightarrow{\text{I.P. } k=2}$ (pokud $p \mid (ab)$, pak $p \mid a$ nebo $p \mid b$), tedy buď $p \mid a_1$ nebo $p \mid (a_2 \dots a_k \cdot a_{(k+1)}) \Rightarrow$ tato část ale říká, že p dělí součin k čísel \rightarrow dle I.P. p dělí některé z $a_2, \dots, a_{(k+1)}$

I.K. ověřen \triangleleft □

15. Formulujte a dokažte základní větu aritmetiky. Při důkazu můžete použít Eukleidovo lemma.

Věta: Každé $n \in \mathbb{N}$, $n \geq 2$ se dá jednoznačně vyjádřit ve tvaru:

$$n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_k^{\alpha_k} = \prod_{i=1}^k p_i^{\alpha_i},$$

kde $k \in \mathbb{N}$, $p_1 < p_2 < \cdots < p_k$ jsou prvočísla a $\alpha_1, \dots, \alpha_k \in \mathbb{N}$
(Tento zápis se nazývá prvočíselným rozkladem čísla n)

Důk: Indukcí: ZK: pro $n=2$ tvrzení triviálně platí. (2 je prvočíslo)
IK: Předpokládáme platnost pro $\forall x \in \mathbb{N}$: $2 \leq x \leq n-1$. Pak n buď prvočíslo (hotovo), nebo složené č. Potom $\exists a, b \in \mathbb{N}$: $n = a \cdot b$. Tedy a, b buď prvočísla (hotovo), nebo pro ně existuje rozklad: $a = p_1 \cdots p_m$ a $b = q_1 \cdots q_n \Rightarrow n = p_1 \cdots p_m \cdot q_1 \cdots q_n$. Tedy existuje rozklad i pro n .
Na základě ZK a opakováním IK platí pro $\forall m \in \mathbb{N}$: $2 \leq m$.
(*I.P. $\rightarrow a, b$ určitě menší než n , tedy pro ně věta platí.)

Ukažme jednoznačnost tohoto rozkladu. \rightarrow sporem
Předpokládejme, že existuje přirozené číslo, které má 2 různé prvoč. rozklady a necht' n je nejmenší takové
Potom předpokládáme existenci $n \in \mathbb{N}$ a prvočísel $p_1, \dots, p_k, q_1, \dots, q_\ell$ takových, že $n = p_1 \cdots p_k = q_1 \cdots q_\ell$
 \Rightarrow tyto faktORIZACE at' jsou různé a pro všechna x taková, že $1 < x < n$ mají faktORIZACI JEDINOU

\hookrightarrow z rovnosti tedy $p_1 | q_1 \cdots q_\ell \Rightarrow$ a podle Eukleidova lemmatu tedy i dělí nějaké q_j
 \Rightarrow BÚNO zvolme $j=1$ (tedy q_1). Ze vztahu dvou prvočísel p_1, q_1 ovšem nutně platí $p_1 = q_1$ a rovnici lze zkrátit na:

$$\frac{n}{p_1} = p_2 \cdots p_k = q_2 \cdots q_\ell$$

Našli jsme tedy číslo ostře menší než n , které má dvě různé faktORIZACE \Rightarrow spor □

16. Formulujte větu o krácení v modulu a dokažte ji. Při důkazu můžete využít toho, že $(\gcd(a, b) = 1 \wedge a|bc) \Rightarrow a|c$.

Věta: Necht' $a, b, c \in \mathbb{Z}$ a $m \in \mathbb{N}$, $m \geq 2$, označme $\underline{d} = \gcd(m, c)$.
Pak platí ekvivalence:

$$ac \equiv bc \pmod{m} \Leftrightarrow a \equiv b \pmod{\frac{m}{d}}$$

Dk: Levá strana $ac \equiv bc \pmod{m}$ je ekvivalentní s $m | (ac - bc)$, to dále rozepíšeme jako:

$$(\exists k \in \mathbb{Z})(c(a-b) = k \cdot m)$$

Dokažeme, že * je ekvivalentní $a \equiv b \pmod{\frac{m}{d}}$

" \Rightarrow " Pokud vyčleníme obě strany rovnosti v * číslem \underline{d} ,
pak získáme: $\left(\frac{c}{\gcd(m, c)}\right)(a-b) = \left(k \cdot \left(\frac{m}{\gcd(m, c)}\right)\right)$

S využitím lemmatu " $\gcd\left(\frac{a}{\gcd(a, b)}, \frac{b}{\gcd(a, b)}\right) = 1$ pro $a, b \in \mathbb{Z}$ "
navíc platí: $\gcd\left(\frac{m}{\gcd(m, c)}, \frac{c}{\gcd(m, c)}\right) = 1$

Jelikož pak $\frac{m}{\gcd(m, c)}$ dělí součin na levé straně
a zároveň nesoudělný s $\frac{c}{\gcd(m, c)}$, nutně musí
platit $\frac{m}{\gcd(m, c)} | (a-b)$, t.j.:

$$a \equiv b \pmod{\frac{m}{\gcd(m, c)}}$$

" \Leftarrow " Necht' platí $\frac{m}{\gcd(m, c)} | (a-b)$, neboli:

$$(\exists l \in \mathbb{Z})(a-b = l \cdot \frac{m}{\gcd(m, c)})$$

Vynásobením obou stran rovnice \underline{c} dostaneme:

$$ac - bc = m \cdot \frac{l \cdot c}{\gcd(m, c)},$$

kde zlomek vpravo je celé číslo. Tedy \underline{m} dělí
 $ac - bc$, což odpovídá * a tvrzení platí. \square

17. Formulujte a dokažte malou Fermatovu větu. Při důkazu můžete použít větu o krácení v modulu.

Věta: Bud' p je prvočíslo a $a \in \mathbb{N}$ takové přirozené číslo, které není násobkem p ($\gcd(a, p) = 1$). Potom platí:

$$a^{p-1} \equiv 1 \pmod{p}$$

Důk: Uvažujme $(p-1)$ celých čísel ve tvaru $j \cdot a$ ($j \in \{1, \dots, p-1\}$), tedy $a, 2a, \dots, (p-1) \cdot a$. Žádné z těchto čísel není dělitelné p , neboť a není násobkem p a $j < p$.

Žároveň, žádná dvě z těchto čísel nejsou navzájem kongruentní mod $p \Rightarrow$ sporum

\hookrightarrow Předpokládejme, že $ka \equiv la \pmod{p}$, kde $1 \leq k < l \leq p-1$.

Potom vzhledem k $\gcd(a, p) = 1$ a větě o krácení v modulu platí $k \equiv l \pmod{p} \Rightarrow$ není možné kvůli $1 \leq k < l \leq p-1$

Tedy ani jedno z $a, 2a, \dots, (p-1)a$ není kongruentní modulo p s 0 a žádné dvě nejsou kongruentní mezi sebou modulo p

\rightarrow jelikož jich je $p-1$, musí jejich nezáporné zbytky modulo p tvořit nějakou permutaci čísel $\{1, 2, \dots, p-1\}$

\hookrightarrow z toho plyne: $a \cdot 2a \cdots (p-1)a \equiv 1 \cdot 2 \cdots (p-1) \pmod{p}$
 $a^{p-1} (p-1)! \equiv (p-1)! \pmod{p}$
 $a^{p-1} \equiv 1 \pmod{p}$

(poslední úprava validní díky $\gcd((p-1)!, p) = 1$)



18. Formulujte a dokažte Čínskou větu o zbytcích. Při důkazu můžete použít toho, že kongruence $MX \equiv 1 \pmod{m}$ má řešení X právě tehdy, když $\gcd(m, M) = 1$.

Věta: Uvažujme soustavu lineárních kongruencí

$$x \equiv a_1 \pmod{m_1}$$

$$x \equiv a_2 \pmod{m_2}$$

\vdots

\vdots

$$x \equiv a_N \pmod{m_N},$$

kde $m_1, m_2, \dots, m_N \geq 2$ jsou navzájem nesoudělná, tedy $\gcd(m_i, m_j) = 1$ pro každá $i \neq j$

Řešení této soustavy vždy existuje a všechna řešení jsou kongruentní modulo M (tedy v \mathbb{Z}_M řešení jednoznačné), kde:

$$M = \prod_{i=1}^N m_i$$

Důk. Ukážeme, že taková soustava je řešitelná.

→ pro každé $i \in \{1, 2, \dots, N\}$ definujeme $M_i := \frac{M}{m_i}$

(tedy součin všech modulů m_j kromě i -tého)

→ klíčové jsou kongruence ve tvaru $M_i X_i \equiv 1 \pmod{m_j}$

"hledání inverze k velkému modulu M_i v malém modulu m_j "

→ pro každé $i \in \{1, \dots, N\}$ platí $\gcd(m_i, M_i) = 1$, potom

$$M_i X_i \equiv 1 \pmod{m_j} \rightarrow X_i \text{ jednozn.}$$

→ pro všechna $j \neq i$ platí (i díky $\gcd(M_i, m_j) = 1$)

$$M_i X_i \equiv 0 \pmod{m_j}$$

⇒ Tvrdíme, že řešení soustavy je:

$$x \equiv a_1 \cdot M_1 \cdot X_1 + a_2 \cdot M_2 \cdot X_2 + \dots + a_N \cdot M_N \cdot X_N \pmod{M}$$

↳ Bud' $j \in \{1, \dots, N\}$ libovolné, zkontrolujeme, zda x splňuje j -tou kongruenci $x \equiv a_j \pmod{m_j}$

$$x \equiv \underbrace{a_1 M_1 X_1}_{\equiv 0 \pmod{m_j}} + \underbrace{a_2 M_2 X_2}_{\equiv 0 \pmod{m_j}} + \dots + \underbrace{a_j M_j X_j}_{\equiv 1 \pmod{m_j}} + \dots + \underbrace{a_n M_n X_n}_{\equiv 0 \pmod{m_j}}$$

$$x \equiv a_j \pmod{m_j} \checkmark$$

Jednoznačnost: Necht' existují $x, y \in \mathbb{Z}_M$ splňující zadanou soustavu. Pro každé $j \in \{1, \dots, N\}$ tedy platí $x \equiv y \pmod{m_j} \Leftrightarrow m_j \mid x - y$, tedy $x - y$ je celočíselným násobkem jejich součinu, a to je právě M . Tedy x a y nutně kongruentní modulo M a v \mathbb{Z}_M existuje jediné řešení. □