

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

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

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

$$E \vee F \vdash \neg(\neg E \wedge \neg F) \rightarrow \text{dle De Morganových zákonů}$$

$$E \Rightarrow F \vdash \neg E \vee F \vdash \neg(\neg E \wedge \neg F) \rightarrow \text{zlaté pravidlo + De Morg.}$$

$$E \Leftrightarrow F \vdash (E \Rightarrow F) \wedge (F \Rightarrow E) \vdash \neg(\neg E \wedge \neg F) \wedge \neg(\neg F \wedge \neg E) \rightarrow \square$$

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

$$E \wedge F \vdash \neg(\neg E \vee \neg F) \rightarrow \text{dle De Morganových zákonů}$$

$$E \Rightarrow F \vdash \neg E \vee F \rightarrow \text{dle zlatého pravidla}$$

$$E \Leftrightarrow F \vdash (E \Rightarrow F) \wedge (F \Rightarrow E) \vdash (\neg E \vee F) \wedge (\neg F \vee E) \vdash$$

$$\vdash \neg(\neg(\neg E \vee F) \vee \neg(\neg F \vee E)) \rightarrow \text{oboje} \quad \square$$

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

Definice: injektivita: Nechť 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: Nechť 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 $f \circ g$ ($f \circ g: A \rightarrow C$)

↳ 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 v $f \circ g$ pro každý prvek $z \in C$ existuje právě jeden vzor $z \in A$ (a množina B slouží jako "prostředník"). □

4. Uvedte, 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:

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

Dоказat: Z definice maticového nasobení 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: ($X = \{x_1, \dots, x_n\}$)

$$(M_{R \circ R})_{i,j} = 1 \Leftrightarrow x_i (R \circ R) x_j \Leftrightarrow (\exists x_k \in X)(x_i R x_k \wedge x_k R x_j)$$

$\hookrightarrow (M_R^2) \Leftrightarrow (\exists k \in \{1, \dots, n\})(M_{R,i,k} = 1 \wedge M_{R,k,j} = 1)$

Ukažme také, když $(MR)_{i,j} \geq 1$. To nastane v takovém případě, když se v sumě dle definice maticového nasobení 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 \square

5. Bud' 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 ekv.: je taková binární relace R na množině X , která je reflexivní, symetrická, transitivní $(\Delta_X \subseteq R \subseteq X \times X) \wedge (R'' = R) \wedge (R^2 \subseteq R)$

Definice třídy - prvku: Nechť R relace na množině X . Pro každé $a \in X$ definujeme třídu prvku a v relaci R jako podmnožinu $[a]_R := \{x \in X \mid xRa\}$

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

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

$$x \in [a]_R \Rightarrow xRa \stackrel{aRb}{\Rightarrow} (xRa \wedge aRb) \stackrel{TR}{\Rightarrow} xRb \Rightarrow x \in [b]_R$$

** Nechť $\neg(aRb)$, pro spor předpokládejme $[a]_R \cap [b]_R \neq \emptyset$, tedy $\exists x \in X$, pro které $xRa \wedge xRb$, potom ale $(xRa \wedge xRb) \stackrel{sy}{\Rightarrow} (aRx \wedge xRb) \stackrel{TR}{\Rightarrow} aRb \rightarrow$ spor a $[a]_R \cap [b]_R = \emptyset$ \square

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

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

Zároveň budete $1 \leq i_1 < i_2 < \dots < i_k \leq n$, 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 zifikovaných, všech permutací ostatních objektů je $(n-k)!$

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

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

\hookrightarrow z definice PIE

Tedy $D_n = n! - \sum_{k=1}^m (-1)^{k-1} \frac{n!}{k!} = \frac{n!}{0!} + \sum_{k=1}^m (-1)^k \cdot \frac{n!}{k!} = \sum_{k=0}^m \frac{(-1)^k n!}{k!} =$

$$= n! \cdot \sum_{k=0}^m \frac{(-1)^k}{k!}$$

□

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 cyklu

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

↳ pro libovolné $m, n \in \mathbb{N}$; $2 \leq n \leq m$

Dоказat: Předpokládejme, že značíme počty permutací m -pruhové množiny s libovolným $(1 \leq \xi \leq m)$ počtem cyklů

[Uvažme libovolnou $(m+1)$ -pruhovou množinu M . Chceme určit počet jejich permutací s m cykly. Vybereme si z M libovolný prvek \underline{x} , pro každou hledanou permutaci M pak platí jedna ze dvou disjunktivních možností:

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

2) \underline{x} je v cyklu s více prvků \Rightarrow potom uvažme permutaci zbylých m -pruhů množiny $M \setminus \{\underline{x}\}$ s m cykly. Když rozhodneme, kam \underline{x} vložíme, nestane se pouze vybrat cyklus, kam jej přidáme, ale vybrat přímo jeden z m zbyvajících pruhů, za kterým v nejakém cyklu bude $\Rightarrow m \cdot s(m, n)$ 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 -pruhové množiny na n tříd.

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

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

Dоказat: Předpokládejme, že známe počty rozkladů m -prvkové množiny do libovolného počtu ($1 \leq t \leq m$) 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 $M \Rightarrow m \cdot S(m, n)$ rozkladů

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

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 $\rightarrow (\forall n \in \mathbb{N}_0)(1 \mid n) \text{ a } (n \mid 0)$, to plyně z faktů $1 \cdot n = n$ a $n \cdot 0 = 0$

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

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

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

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

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

\downarrow
 k

AN) Nechť': $(\forall a, b \in \mathbb{N}_0 \setminus \{0\})(a \mid b \wedge b \mid a) \Rightarrow a = b$

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

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

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

\rightarrow pro \mathbb{Z} stačí protipříklad, když $a = -b$

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

Nechť taková a, b, c splňují $a \mid b \wedge b \mid c$, tedy $(\exists \ell \in \mathbb{Z})(a \cdot \ell = b) \wedge (\exists l \in \mathbb{Z})(b \cdot l = c)$

\hookrightarrow z toho prvního plyne $a \cdot (\ell \cdot l) = c \Rightarrow a \mid c$

\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 (délitelnosti)
- $\mathbb{N} \setminus \{1\}$: největší ani maximální prvek/prvek neexistuje
minimální prvek jsou prvocisla, nejmenší není

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

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

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

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

Dk: Indukce: uvažme nejprve existenci $q, r \in \mathbb{Z}$ pro všechna $a > 0$

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

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

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

Pokud ovšem $(r+1) = d$, pak stačí rovnici upravit na $a+1 = q \cdot d + d = (q+1) \cdot d + 0$ ✓

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

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

Pokud $r = 0$, pak $(-q)$ 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 dělitel a zbytek pro všechna $a \in \mathbb{Z}$

Jednoznačnost: Předpokládejme $q_1, q_2, r_1, r_2 \in \mathbb{Z}$ a

$$\underline{a} = q_1 d + r_1 = q_2 d + r_2 \quad \text{a} \quad 0 \leq r_1, r_2 < d, \text{ pak ale} \Rightarrow (q_2 - q_1)d = (r_1 - r_2).$$

Tedy $d | (r_1 - r_2)$, současně ale musí platit $0 \leq |r_1 - r_2| < d \Rightarrow r_1 - r_2 = 0 \Rightarrow q_2 - q_1 = 0 \quad \square$

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:

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

Důkaz: Nechť $\underline{d} = \gcd(a, b)$, chceme ukázat, že $\frac{a}{d}$ a $\frac{b}{d}$ nemají jiný společný (ladný) dělitel než 1

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

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

$$de \leq d$$

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

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:

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

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

Checeme popsat obecné řešení (x,y) . Uvítě potom platí $ax+by = ax_0+by_0 \rightarrow$ tedy $ax - ax_0 = by_0 - by$. Po vydeleníem d získáme:

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

$\Rightarrow \frac{a}{d}$ dělí součin upravo; $\frac{b}{d}$ dělí součin vlevo

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

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

$$\left(\frac{b}{d} \mid \frac{a}{d}(x-x_0) \wedge \gcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1 \right) \Rightarrow \frac{b}{d} \mid (x-x_0)$$

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 přeznačme $k=u=v$)

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:

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

□

13. Kolik existuje prvočísel? Své tvrzení dokažte.

Tvrzení: Existuje nekonečné mnoho prvočísel.

Dоказ: Sporem \rightarrow předpokládáme konečné mnoho různých prvočísel $1 < p_1, p_2, p_3, \dots, p_k$ (veškerá prvočísla)

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

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

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

Tedy $p_j | P$, ale i $p_j | p_1 \cdot p_2 \cdots p_k$

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

Zde se dá odkažat na tvrzení:

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

\Rightarrow zvolime tedy $b = P$, $c = p_1 \cdot p_2 \cdots p_k$, $m = 1$, $n = 1$
 $a = p_j$, potom ale ze vztahu * plyne, že musí platit $p_j | 1 \Rightarrow$ spor s *

\Rightarrow Prvočísel je nekonečné 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 $p \mid (a_1 \cdot a_2 \cdots a_k)$, kde $a_i \ (i \in \{1, \dots, k\})$ jsou přirozená čísla, pak existuje $1 \leq j \leq k$ takové, že $p \mid a_j$

Dk: 1) Bezantova rovnost máme pro dvě nesoudělná čísla (a, p) zaručuje existenci x, y takových, že $px + ay = 1$. Tuto rovnost rozšíříme o b , tedy máme $pxb + aby = b$. Zjistíme, že p dělí oba sčítance vlevo ($p \mid ab$) \Rightarrow tedy musí dělit i jejich součet $\Rightarrow p \mid b$.
 $(ab \wedge ac) \Leftrightarrow (\exists m, n \in \mathbb{Z})(a \mid (m \cdot b + n \cdot c))$

2) Indukci podle $k \in \mathbb{N}$ s využitím bodu 1)

ZK: $k=1 \Rightarrow$ zjistíme, že platí "pokud $p \mid a$, pak $p \mid a$ ".
 $k=2 \Rightarrow$ plyne z bodu 1)

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

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

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

$\stackrel{\text{I.P. } k=2}{\Rightarrow} (\text{pokud } p \mid (ab), \text{ pak } p \mid a \text{ nebo } p \mid b), \text{ tedy bud' } p \mid a,$
 $\text{nebo } p \mid (a_2 \cdots a_k \cdot a_{(k+1)}) \Rightarrow$ 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 \square

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)

Dk: Indukce: ZK: pro $n=2$ tvrzení trivialně platí. (2 je prvočíslo)

IK: Předpokládáme platnost pro $\forall x \in \mathbb{N}: 2 \leq x \leq n-1$. Pak \underline{n} budí prvočíslo (hotovo), nebo složené č. Potom $\exists a, b \in \mathbb{N}: n = a \cdot b$. Tedy a, b budí 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 $\forall n \in \mathbb{N}: 2 \leq n$.
(*I.P. $\rightarrow a, b$ určitě menší než \underline{n} , tedy pro ně věta platí.)

Ukážeme jednoznačnost tohoto rozkladu. \rightarrow sporem
Předpokládáme, že existuje přirozené číslo, které má 2 různé prvoč. rozklady a nechť \underline{n} je nejmenší takové.
Potom předpokládáme existenci $\underline{m} \in \mathbb{N}$ a prvočísel $p_1, \dots, p_k, q_1, \dots, q_\ell$ takových, že $\underline{n} = p_1 \cdots p_k = q_1 \cdots q_\ell$
 \Rightarrow tyto faktorizace at. jsou různé a pro všechna x taková, že $1 < x < \underline{n}$ mají faktorizaci jedinou

\hookrightarrow z rovnosti tedy $p_1 q_1 \cdots q_\ell \Rightarrow$ a podle Eukleidova lemmatu tedy i delí nejare 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:

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

Našli jsme tedy číslo ostře menší než \underline{n} , které má dvě různé faktorizace \Rightarrow spor □

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

Veta: Nechť $a, b, c \in \mathbb{Z}$ a $m \in \mathbb{N}$, $m \geq 2$, označme $\underline{d} = \underline{\gcd}(m, c)$.
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 dale rozepíšeme jako:

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

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

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

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 nesoudebný 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 " Nechť platí $\frac{m}{\gcd(m,c)} | (a-b)$, neboť:

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

Vynásobením obou stran rovnice c dostaneme:

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

kde zlomek upravo 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.

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

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

Dle: 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 $j < p$.

Zároveň, žádná dvě z těchto čísel nejsou navzájem kongruentní mod p \Rightarrow spor.

\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 $l \equiv k \pmod{p} \Rightarrow$ 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 tvorit nějakou permutaci čísel $\{1, 2, \dots, p-1\}$

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

(poslední úprava platí i když $\gcd((p-1)!, p) = 1$)

□

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

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

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

⋮ ⋮

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

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:

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

Dоказat: Ukažeme, 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)

→ křížové jsou kongruenze ve tvare $M_i X_i \equiv 1 \pmod{m_i}$
"hledání inverze k velkému modulu M_i v malém
modulu m_i "

→ pro každé $i \in \{1, \dots, N\}$ platí $\gcd(m_i, M_i) = 1$, potom
 $M_i X_i \equiv 1 \pmod{m_i} \rightarrow X_i$ jednoznačn.

→ pro všechna $j \neq i$ platí (i díky $m_i \mid M_i$)
 $M_i X_i \equiv 0 \pmod{m_j}$

⇒ Vyrovnáme, 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 -tu kongruenci $x \equiv a_j \pmod{m_j}$

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

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

Jednoznačnost: Nechť existují $x, y \in \mathbb{Z}_M$ splňující zadанou soustavu. Pro každé $j \in \{1, \dots, N\}$ tedy platí $x \equiv y \pmod{m_j} \Leftrightarrow m_j | x - y$, tedy $\underline{x-y}$ je celocíselným násobkem jejich součinu, a to je právě M . Tedy x a y nutně kongruentní modulo M a v \mathbb{Z}_M existuje jedinečné řešení. \square