1. **Konjukcia.**

   Jupitér je planéta a Slnko Hviezda. Vonka sneží a je chladno. (a, a súčasne)

p q	pAq	negácia(pAq)
11	1	0
10	0	1
01	0	1
00	0	1

   negácia: znegujem oba výrazy a pridám spojku alebo. Vonka nesneží alebo nie je chladno.

2. **Disjunkcia.**

   Vonka sneží alebo je mráz. (alebo)

pq	pVq	negáciac(pVq)
11	1	0
10	1	0
01	1	0
00	0	1

   Vonka nesneží a nie je mráz.

3. **Implikácia**

   Ak vonku prší ulice sú mokré. (ak, tak)

pq	p=>q	negácia(p=>q)
11	1	0
10	0	1
01	1	0
00	1	0

   negácia: ak prvú jej zložku necháme nezmenenú a druhú zložku znegujeme a zložky spojíme spojkou a. Prší a ulice nie sú mokré. Žilina vyhrá a ja nezjem kefu.

4. **Ekvivalencia**

   Naše mužstvo postúpi práve vtedy, keď vyhrá zápas (práve vtedy, vtedy a len vtedy keď)

pq	p⇔q	negácia(p⇔q)
11	1	0
10	0	1
01	0	1
00	1	0

   Naše mužstvo postúpi a nevyhrá zápas alebo vyhráme zápas a naše mužstvo nepostúpi.

5. **Existenčný E naopak a všeobecný kvantifikátor A naopak**

   existenčný(niektorý, aspoň jeden). Keď chceme vyjadriť, že určitú vlastnosť môžu mať objekty z nejakého súboru objektov(z nejakej množiny) napr. Existuje aspoň jeden chlapec ktorý má čierne vlasy.

   všeobecný: (každý, všetci). Keď chceme vyjadriť, že všetky objekty z nejakého vymedzeného súboru objektov(z nejakej množiny) majú daný vlastnosť

   negácia: zmení sa existenčný na všeobecný a zneguje sa vlastnosť naopak.

   Niektorá profesori sú holohlavý – negácia: Všetci profesori majú vlasi.

6. **Čo to znamená, že množina A je podmnožinou množiny B**

   Množina A je podmnožinou množiny B, ak každý prvok množiny A je práve aj prvok množiny B. A={1,2,3} B={0,1,2,3,4}

   karteziánsky súčin: AxB množín A a B je množina všetkých usporiadaných dvojíc, kde prvý prvok dvojice je z množiny A a druhý prvok tejto dvojice je z množiny B.

AxB={(x,y)}|x e A, y e B}

rozklad množiny: Množiny A_1, $A_{2....}A_k$ tvoria rozklad množiny A, ak A = A1 U A2 U...UA_k a zároveň pre ∀i, j e {1,…,k} (i sa nerovná j) platí Ai prienik Aj = prázdnej množine

množina všetkých podmnožín: Ak A = {1,2}, tak zo všetkých podmnožín tejto množiny môžeme vytvoriť novú množinu, nazývame ju potečná množina: P(A) = {Ø,{1},{2},{1,2}}

7. **Zjednotenie, prienik, rozdiel a symetrickú diferenciu množín.**

Prienik: A∩B množín A a B obsahuje práve tie prvky, ktoré patria do množiny A a zároveň B.

Zjednotenie: AUB množín A a B obsahuje tie prvky, ktoré patria do množiny A alebo B.

Rozdiel: A-B množín A a B obsahuje práve tie prvky, ktoré patria do množiny A a zároveň nepatria do B.

Symetrická diferencia: AΔB množín A a B obsahuje tie prvky, ktorí patria práve do jednej z množín A, B.

8. **Rekurzívne definované množiny**

Definujeme množinu A nasledovne:

1., základný krok definície: x1,x2,xk eA

2., konštrukčné kroky: ak y1,z2,…yl eA => z1, z2....zm eA.

kde prvky z1,z2,....zm vytvárame z prvkov y1,y2...yl pomocou pevne daných pravidiel.

príklad: 1. 0eA, 2. ak neA =>(-n eA Λ n+2 eA).

9. **Definujte binárne relácie z množiny A do množiny B.**

reflexívna – ak pre ∀x e A xRx **symetrická** ak V x,y e A je nasledujúci výrok pravdivý: ak xRy => yRx **antisymetrická:** ak pre V x,y eA je nasledujúci výrok pravdivý: ak xRy a súčasne yRx => x=y **tranzitívna**: ak pre V x,y,z e A je nasledujúci výrok pravdivý: ak xRy a súčasne yRz => xRz.

10. **Relácia ekvivalencia a čiastočného usporiadania**

Relácia R c AxA je reláciou ekvivalencie, ak je reflexívna, symetrická, tranzitívna.

Relácia R c AxA je čiastočným usporiadaním, ak je reflexívna, antysimetrická, tranzitívna.

11. **Zvoľte si prirodzené číslo a prevedte ho do sústavy**

$37 = 1.2^5+0.2^4+0.2^3+1.2^2+0.2^1+1.2^0(100101)$

$2589 = 10(A).16^2+1.16^1+13(C).16^0$ (A1D)

$2589 =1.11^3+10.11^2+4.11^1+4.11^0$ (1X44).

Ak $x = (a_k, a_{k-1},...a_1,a_0)z$ potom $x = a_kz^k+a_{k-1}z^{k-1}+\ldots+a_2z^2 + a_1z^1 + a_0z^0$

12. **Opíšte princíp matematickej indukcie**

Množinu prirodzených čísel N možno definovať rekurzívne nasledujúcim spôsobom:
1., základný krok definície: 1e N 2., konštrukčné kroky: ak n eN => n+1 e N.
Indukcia nám hovorí, že takto možno generovať každý prvok množiny prirodzených čísel. Tento fakt možno využiť ako jednu z metód dokazovania. Ide o princíp matematickej indukcie.

13. **Opíšte dva spôsoby kódovania celých čísle na počítači.**

prvý spôsob: zapísať priamy kód, kde vyjadríme najprv absolútnu hodnotu a potom pridáme najvyšší byt ktorý znamená znamienko daného čísla 0 kladná a 1 záporná
8bit číslo 0(+)1001101, nefungujú pri ňom aritmetické operácie.

druhý spôsob: dvojkový doplnok: kladné čísla zapisujeme rovnako ako v priamom kóde a záporné čísla: všetky 0(aj znamienko) zmeníme na jednotky a jednotky zas na nuly a k číslu pripočítame jednotku
napr. 49 – (00110001) – (11001110) + 1 – (11001111)
Pri súčte (1111)+(0001) =(10000) si treba uvedomiť, že máme na reprezentáciu len 4bitové čísla a v tejto reprezentácii ten súčet vyzerá nasledovne: (0000)

14. **Racionálne čísla**
Prvé zmienky o racionálnych číslach možno nájsť už v starovekom Egypte a Mezopotánii. Racionálne čísla sú čísla, ktoré vieme zapísať v tvare zlomku a/b kde a,b e Z, b je rôzne od nuly. Označujeme ich Q.
napr. 3/8 v dvojkovej sústave musíme toto číslo previesť na tvar: $a_1.2^{-1}+a_2.2^{-2}+a_3.2^{-3}+...$ Potrebujeme zistiť hodnotu číslic a1,a2,a3...vynásobíme z číslom 2.... $2z=a_1.2^0 + a_2.2^1...$ Číslica a1 sa dostala pred desatinnú čiarku a preto nie je problém ju zistiť. Takto môžeme posúvať číslice postupne za desatinnú čiarku.
pr. $z = 0,625$ $2z = 1.25$ – $a_1 = 1$
$z_1 = 0,25$ $2z_1 = 0,5$ - $a_2 = 0$
$z_2 = 0,5$ $2z_2 = 1,0$ - $a_3 = 1$
$z_3 = 0,0$ čiže 0,625 = (0,101)

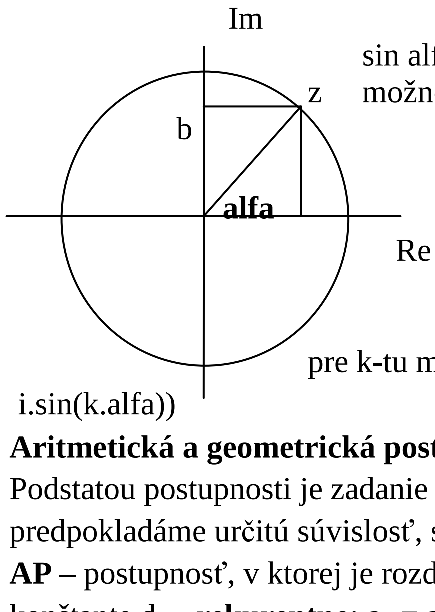
1. spôsob

15. **Dokážte že odmocnina z dvoch nie je racionálne číslo**
Odmocnina z dvoch nie je racionálne číslo lebo sa nedá napísať v tvare zlomku a/b
Dôkaz – sporom. Predpokladajme, že odmocnina z dvoch je racionálne číslo, a dá sa napísať v tvare zlomku a/b kde a,b eZ, b je rôzne od nuly. Predpokladajme, že zlomok a/b je už upravený na základný tvar. Potom $2 = a^2/b^2$ a $a^2 = 2b^2$. Čiže a^2 je párne číslo. Potom aj a je párne číslo. Potom existuje x eN také, že a = 2x. Potom $a^2 = 4x^2 = 2b^2$ a tiež $b^2 = 2x^2$. Podobne ako pre a platí, že b musí byť párne. Čiže existuje yeN také, že b = 2y. To je v rozpore s predpokladom, že a/b je zlomok v základnom tvare, pretože sa dá zjednodušiť dvojkou: a/b = 2x.x/2y.y.
Mohli by sme povedať, že a/b nie je už v základnom tvare, ale x/y už áno. Lenže x/y sa dá tiež zjednodušiť dvojkou atď až do nekonečna. Takže musí platiť pôvodné tvrdenie.

16. **Komplexné čísla**
Sú čísla v tvare a+b.i, kde a,b eR a i = odmocnina -1 : imaginárna jednotka.
odmocnina -1 nie je reálne číslo. $i^2 = -1$
veľkosť komplexného čísla z = a+bi vypočítame |z| = odmocnina z a^2+b^2
komplexne združené ż = a-bi a z=a+bi kde platí $z.ż = c^2 + d^2 = |z|^2$

(a+bi) + (c+di) = (a+c) + (b+d)i (a+bi) - (c+di) = (a-c) + (b-d)i
(a+bi) . (c+di) = (ac - bd) + (ad + bc)i (a+bi) : (c+di) = (ac-bd)+(bc-ad)i/$c^2 + d^2$

17. **Komplexné čísla goniometrický tvar**
Nech je dané komplexné číslo z = a+bi



sin alfa = b/|z| a cos alfa = a/|z|. Takže komplexné číslo možno vyjadriť vyjadriť v tvare z = |z|.(cos alf. + i.sin alf.)

pre: $z_1 = |z_1|$.(cos alf. + i.sin alf.) a z_2 =
$z_2 = |z_2|$.(cos alf. + i.sin alf.)
*: z1.z2 =|z1|.|z2|(cos(alf + beta)+i.sin(alf + bet))
: z1/z2 = |z1|/|z2|(cos(al - bet) + i.sin(alf - beta))

pre k-tu mocninu (kde k eR): $z_1^k=|z_1|^k$(cos(k. alfa) + i.sin(k.alfa))

18. **Aritmetická a geometrická postupnosť**
Podstatou postupnosti je zadanie usporiadanej sekvencie R čísel u ktorých predpokladáme určitú súvislosť, spoločný význam
AP – postupnosť, v ktorej je rozdiel každých dvoch po sebe idúcich členov sa rovná konštante d. **rekurentne:** $a_n = a_{n-1} + d$ **vzorcom**: $a_n = a_1 + (n-1).d$

GP – postupnosť, v ktorej podiel každých dvoch po sebe idúcich členov sa rovná konštante q. **rekurentne:** $a_n = a_{n-1} . q$ **vzorcom:** $a_n = a_1 . q^{n-1}$

19. **Rastúca, klesajúca, nerastúcej, neklesajúcej, zhora ohraničenej**

rastúca: Vn eN: $a_{n+1} > a_n$ 1,2,3,4… **neklesajúca:** V n eN: $a_{n+1} \geq a_n$ 1,2,3,4 a 1,1,2,2.
klesajúca: V neN $a_{n+1} < a_n$ 1,1/2.. **nerastúca**: VneN $a_{n+1} \leq a_n$ -1,-1,-2,-2...
ohraničená: dola: Ey eR VneN $a_n \geq y$ z hora: ExeR VneN $a_n \leq x$

20. **Hromadný bod postupnosti**

jeden HM {1/n } **dva hromadné body: $\{(-1)^n\}$** HB: (-1,1)

21. **Limita postupnosti**

Ak má postupnosť $\{a_n\}^{\infty}_{n=1}$ práve jeden hromadný bod @ ktorý môže byť reálne číslo, alebo +-∞, potom hovoríme, že má limitu @. Limita je odhad ako sa postupnosť bude správať do +-∞. ~~Pre GP: ak q>1: lim je ∞, q = 1: lim = a_n – postupnosť je konštantná, q e<0,1>: lim = 0 a ak je q<0 lim: neexistuje.~~

22. **Vzorec pre súčet AP a GP**

$a_1+a_2+....a_k+.........+a_n = Sn$ $(a_1+a_n).n = 2.Sn$: $Sn = \frac{(a_1+a_n).n}{2}$
$a_n+a_{n-1}....a_{n-k+1}+...+a_1 = Sn$
$2a_1+(n-1).d$

$a_2=a_1+d$ $a_k=a_1+(k-1).d$
$a_{n-1}=a_1+(n-2).d$ $a_{n-k+1}=a_1+(n-k).d$
$a_2+a_{n-1}=2a_1+(n-1)$ $2a_1+(n-1).d$

GP: $Sn = a_1+a_2+......a_n = a_{1+}\ a_1.q+ a_1q^2.... a_1.q^{n-1}= a_1.(1+q+q^2+...+q^{n-1})$
$S´n=1+q+q^2+...+q^{n-1}/(-q)$ => $-qS´n = -q -q^2-...-q^{n-1}-q^n$
$S´n-q.S´n = 1- q^n$ $S´n.(1-q)=1-q^n$ .... ak q sa nerovná 1 tak $S´n = \frac{1-q^n}{1-q}$ **$Sn = a_1.\frac{1-q}{1-q}$**

23. **Sumovateľnosť**

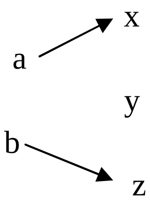
Za súčet členov nekonečnej postupnosti považujeme limitu postupnosti čiastkových súčtov lim Sn, ak existuje a je rovná reálnemu číslu. Ak postupnosti čiastkových súčtov postupnosti $\{a_n\}^{\infty}_{n=p}$ má limitu rovnú reálnemu číslu , tak hovoríme, že táto postupnosť je sumovateľná. Ak spomenutá limita neexistuje, alebo je rovná +-∞, tak hovoríme, že postupnosť nie je sumovateľná.

24. **Funkcia z množiny A do množiny B**

25. **Injektívna, surjektívna a bijektívna funkcia**

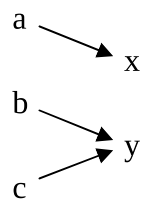
Injektívna: Ak zobrazenie f: $A \rightarrow B$ priradí každej dvojici navzájom rôznych prvkov z množiny A dva rôzne prvky z množiny B, tak hovoríme, že f je prostá

napr. **ŠPZ**, dve rôzne autá nemôžu mať jednu rovnakú špz-tku.

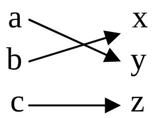


Surjektívna: Ak ku každému prvku y z množiny B existuje prvok x množiny A taký, že f(x)=y, potom túto funkciu nazývame surjektívna.

pr. dvaja rôzny ľudia môžu mať rovnaký dátum narodenia.



Bijektívna funkcia je taká, ktorá je súčasne injektívna a aj surjektívna.



26. **Čoho je viac? Prirodzených čísel alebo reálnych čísel?**

Keďže sa bavíme o nekonečnej množine R a N čísel budeme hovoriť o mohutnosti množín. (nakresli os) Existuje injekcia z N do R, ale zároveň neexistuje bijekcia a z toho vyplýva že N má menšiu mohutnosť ako R(|N|<|R|).

27. **Čoho je viac? Konečných programov alebo funkcií z N do N?**

Určite je viac funkcií z N do N. Množinu programov označme P. Každý program vieme zapísať ako postupnosť núl a jednotiek a každej takejto postupnosti vieme priradiť prirodzené číslo. Navyše to priradenie vieme uskutočniť tak, že rôznym programom priraďujeme rôzne čísla, čiže máme injekciu z P do N.

platí teda $|P| \leq |N| < |\langle 0,1)| \leq |F|$.

To znamená, že všetkých programov, ktoré vieme zapísať, je menej ako funkcií z N do N. Takže je možné medzi nimi nájsť také funkcie, pre ktoré neexistuje konečný program, ktorý pre ľubovoľný vstup vypočíta funkčnú hodnotu. Čiže ani funkcie z N do N nie sú všetky vypočítateľné.

28. **Čoho je viac? podmnožín n-prvkovej triedy alebo usporiadaných n-tíc.**

Je ich rovnako, keď počítame n-tice {0,1} v k-cifernom čísle, na každej jeho pozícii môže byť 0 alebo 1, čiže 2 možnosti na každom mieste, to je 2^n. Všetkých podmnožín n-prvkovej množiny je tak isto 2^n.

29. **Výpočtová zložitosť O(f(n))**

O-notácia sa používa na vyjadrenie výpočtovej zložitosti algoritmov. Výpočtová zložitosť znamená počet krokov, ktoré musí v najhoršom prípade algoritmus vykonať.

Nech sú dané funkcie f: $N \longrightarrow R^+$ a g: $N \longrightarrow R^+$. Hovoríme, že f(n) = O(g(n)), ak existuje konštanta c > 0 a n_0 e N take, že pre VneN. $n \geq n_0$ platí $f(n) \leq cg(n)$.

Počítač dokáže spracovať 10^{10} operácií za sekundu.

g(n)\n	500
n^2	25ms
2^n	-
n!	-

nie sú z praktického hľadiska veľmi výhodné, pretože doba výpočtu pre väčšie n je neúnosná. Z toho vyplýva, že algoritmy so zložitosťou O(n!) a $O(2^n)$ nie sú vhodné pre praktické použitie.

30. **Ktorá funkcia rastie rýchlejšie ?**
31. **....**
32. **Dokážte, že reláciu delí na množine...**
33. Nevypracované.
34. **Euklidov algoritmus**

Nájdime NSD čísel 276 a 120. Vyjadrujeme postupne zvyšky:

276 = 2.120 + 36

120 = 3.36 + 12

36 = 3.12 + 0

Posledný nenulový zvyšok je najväčším spoločným deliteľom čísel 276 a 120.

Všeobecne: NSD čísiel a a b. Predpokladajme, že a > b. Postupne vyjadrujeme zvyšky, ako v predchádzajúcom príklade:

$a = q_1.b + r_1$

$b = q_2.r_1 + r_2$

$r_1 = q_3.r_2 + r_3$

.

$r_{i-2} = q_i \cdot r_{i-1} + r_i$

$r_{i-1} = q_{i+1} \cdot r_i + 0$

Pre zvyšky platí:

0 < r1 < b

0 < r2 < r1

0 < r3 < r2

...

0 < ri < ri−1 Najväčší spoločný deliteľ čísel a a b je posledný nenulový zvyšok, čiže r_i.

0 = ri+1

35. Prvočísla a zložené čísla

Prvočísla sú čísla ktoré majú pravé dvoch deliteľov a to jednotku a samého seba.

Zložené čísla sú čísla ktoré majú viac ako 2 deliteľov.

Každé prirodzené číslo a > 1 je možné jednoznačne vyjadriť v tvare: $a = p_1.p_2....p_n$, kde p_1 až p_n sú prvočísla a platí, že $p_1^{a1} \leq p_2^{a2} \leq \ldots \leq p_n^{an}$.

36. **Prvočísel je nekonečne veľa.**

Predpokladajme, že toto tvrdenie neplatí a prvočísel je konečne veľa. Označme ich ako $p_1,p_2..p_k$. Nech $P = p_1 . p_2...p_k + 1$. Číslo P nemôže byť prvočíslo, pretože je väčšie ako každé z prvočísel $p_1,p_2..p_k$. Teda P by malo byť zložené číslo, ale potom P musí byť deliteľné prvočíslom. Avšak P dáva po delení ľubovoľným z prvočísel $p_1,p_2..p_k$ zvyšok 1. Takže P nemôže byť ani zložené číslo. Dospeli sme k sporu. Musí platiť pôvodné tvrdenie, čiže prvočísel je nekonečne veľa.

37. **Algoritmus na zisťovanie prvočísel**

1., vypočítaj odmocninu z n

2., pre VxeN, kde xe <2,odmocnina z n> urob: ak x/n, nie je prvočíslo

3., Ak žiadne x nie je deliteľom n potom n je prvočíslo

nie je efektívny v praxi, ak máme číslo 2^{256}, tak musíme otestovať čísla od 2 po 2^{128}.

38. Nevypracované
39. Pre ktoré peN (p>1) sú všetky lineárne rovnice tvaru...

40. **Fermatova veta**

Zápis x ≡ y (mod p) znamená, že čísla x, y dávajú rovnaký zvyšok po delení číslom p. Zápis x ≡ 1 (mod p) môžeme chápať aj tak, že x dáva zvyšok 1 po delení číslom p. Zápis x ≡ y (mod p) čítame: ”x je kongruentne s y modulo p” (nazýva sa aj kongruencia) a ≡ je binárna relácia nazývaná relácia kongruencie.

Existuje zložené číslo...Boli nájdené také zložené čísla (Carmichaelove čísla) pre ktoré

ktoré to platí

41. **Princíp rýchleho umocňovania**

Číslo 17 zapisujeme v dvojkovej sústave $(10001)_2$. Čiže $17 = 2^0 + 2^4$ a $7^{17} = 7^{20+24} = 7^1 \cdot 7^{16}$. Hodnotu 71 mame a 716 vieme vypočítať nasledovne: počítame postupne

$7^2 \rightarrow (7^2)^2 = 7^4 \rightarrow (7^4)^2 = 7^8 \rightarrow (7^8)^2 = 7^{16}$.

To znamená štyri súčiny na výpočet 7^{16} a jeden súčin $7^1 \cdot 7^{16}$. To je spolu 5 súčinov miesto 16.

Dá sa využiť len asociatívnosť súčinu a je preto použiteľný napríklad pre umocňovanie matíc a takto vieme rýchlo umocňovať aj poli Z_p kde p je prvočíslo

42. **Ako vypočítame opačný prvok –u?**

Na hľadanie inverzného prvku môžeme využiť malú Fermatovu vetu. Keďže p je prvočíslo a číslo $a \in Zp = \{0, 1, \ldots, p - 1\}$ (navyše a != 0), tak čísla a, p sú nesúdeliteľné (inak by malo p deliteľa rôzneho od 1 a p a nebolo by prvočíslom). Potom spĺňajú predpoklady malej Fermatovej vety a platí:
$a^{p-1} = a \cdot a^{p-2} \equiv 1 \pmod p$.
Čiže súčin $a \cdot a^{p-2}$ dáva zvyšok 1 po delení číslom p. To však znamená, že $a \odot a^{p-2} = 1$ a $a^{-1} = a^{p-2}$. Vďaka algoritmu na rýchle umocňovanie vieme inverzný prvok vypočítať aj v poli$(Zp, \oplus p, \odot p)$, keď p je veľké prvočíslo.

45. **Turningov stroj**

Ak chceme formálne opísať výpočet hodnôt funkcie. Vstup funkcie môžeme pomocou núl a jednotiek zapísať na vstupnú pásku. Výstup môžeme podobne zapísať na výstupnú pásku. Samotný priebeh výpočtu je charakterizovaný diagramom a postupnosťou stavou, ktoré prechádzame počas výpočtu. Turningov stroj v prvom príklade teda zodpovedá funkcii, ktorá každému slovu vstupe priradí 1 alebo 0. V druhom príklade máme Turingov stroj, ktorý reprezentuje funkciu, ktorú môžeme formálne zapísať:
f: $\{0,1\}^2 \rightarrow \{0,1\}^2$, kde f(00) = 0, f(01) = f(10) = 1, f(11) = 10. Čiže spomenutú funkcie a ich výpočet môžeme reprezentovať pomocou uvedených turingových strojov.