

Matematinės Interneto svetainės



Alfredas Račkauskas

alfredas.rackauskas@mif.vu.lt

Prisėdus prie kompiuterio jau galima ne tik apsipirkti, užsakyti viešbutį, rezervuoti vietą traukinyje ar lėktuve, bet ir pasidairyti po pasaulinio garso muziejus, pasigrožėti garsių dailininkų paveikslais, susipažinti su įvairiausių leidyklų katalogais ir išsirinkti knygą. Gal dar sunku įsivaizduoti, kad Gariūnų turgus taip pat gali turėti savo svetainę adresu gariunai.com, bet norim to ar ne, Internetas skverbiasi į visas gyvenimo sritis.

Straipsnio autorius — VU Matematikos ir informatikos fakulteto profesorius. Jo mokslinio darbo kryptis — tikimybių teorija ir jos taikymai.

Tikriausiai jau nebėra universiteto, kuris Internetu neturėtų savo svetainės. Čia pristatomos studijų programos, pavieniai kursai, doktorantai kviečiami į vasaros mokyklas, siūlomos nuotolinės studijos ir pan. Akademiniame pasaulyje jau išmoko naudotis Interneto teikiama galimybėmis.

O ką įdomaus Internetu gali rasti matematikos mokytojas? Sukurta daugybė Interneto puslapių, kuriuose galima rasti įvairiausių informacijos — tiek metodinės, tiek praktinės. Pamokų planai, mokomieji žaidimai, pagalbinės metodinės priemonės, mokytojų patarimai

mokytojams, diskusijos pamokų vedimo, auklėjimo ir kitais klausimais — visa tai galima rasti Internetu. Atsirado puiki galimybė plėsti akiratį, užpildyti metodikos spragas, kitaip pažvelgti į matematikos pamokas ar matematikos būrelio užsiėmimus.

Kiekviename žurnalo „Alfa plus omega“ numeryje stengsimės pristatyti svetaines, kuriose matematikos mokytojas galėtų rasti sau įdomios ir naudingos informacijos. Tikimės sulaukti mokytojų atsiliepimų apie tų svetainių turinį ir taip pat kritinių pastabų apie jų naudą.



The MacTutor History of Mathematics archive

<http://www.group.dcs.st.and.ac.uk/history/>

Tai matematikos istorijai skirta svetainė. Ją sukūrė Škotijos Šv. Andriejaus universiteto Matematikos ir statistikos mokykla. Svetainė turi keletą skyrelių, kuriuos trumpai ir apžvelgsime.

Skyrelyje *Biographies Index* galime rasti išsamios informacijos apie daugiau nei 1100 ma-

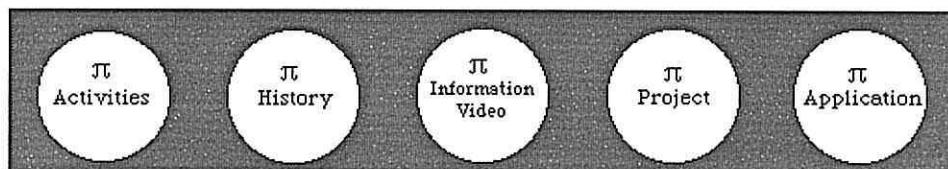
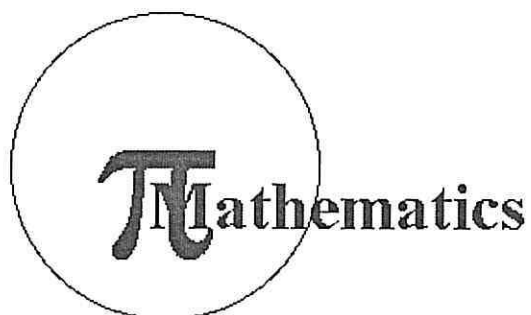
tematikų. Ką šioje svetainėje galima sužinoti, pavyzdžiui, apie Pitagorą? Nueikime į skyrelį *Biographies Index*, pagal raidę P susiraskime *Pythagoras of Samos* ir žvilgtterėkime, kas ten rašoma. Štai keletas ištraukų iš jo biografijos.

Pagal šį tekstą gauname tokius skaičiaus π skaitmenis: 3,14159265358979323846264...

Būtų įdomu, jei kas nors pasiūlytų lietuvišką variantą! Bandykite. Įdomiausius variantus skelbsime.

Beje, yra ir atskira skaičiui π skirta Interneto svetainė — π Mathematics.

Čia apstu pačios įvairiausios informacijos apie skaičių π . Medžiaga skirta 6–8 klasių moksleiviams. Be to, čia rasite pamokų planų, praktinių užsiėmimų aprašymų.



<http://www.ncsa.uiuc.edu:80/edu/RSE/RSEorange/buttons.html>

EAN — šiek tiek matematikos buityje

Jevgenij Volosatov

vev@is.lt

Straipsnyje rašoma apie brūkšninį kodą, kurį kasdien matome ant įvairių prekių. Šis kodas suteikia galimybę skaitančiajam įrenginiui nustatyti, ar kodas perskaitytas be klaidų. Tačiau gali būti ir taip, kad įvykusios klaidos bus nepastebėtos. Ar didelė tokio įvykio tikimybė?

Šio straipsnio autorius — VU Matematikos ir informatikos fakulteto informatikos specialybės studentas.

Šifravimas ir kodavimas

Visi girdėjo žodžius „šifravimas“ ir „kodavimas“. Tačiau ne visi žino, kad tai ne vienas ir tas pats. Pavyzdžiui, jei visas abėcėlės raidės pakeisime kitomis, tarkime, A pakeisime G, N — T, M — U, S — L ir pan., tai žodį NAMAS galėsime šifruoti žodžiu TGUGL. Šifro prasmę galės atskleisti tik žinantys šifro raktą, t. y. raidžių keitimo raidėmis (arba kitais simboliais) taisyklę.

Kodavimo tikslas — ne paslėpti informacijos prasmę nuo pašalinių, bet pertvarkyti ją, kad būtų galima pasiųsti, laikyti ir pan.

Tokio kodo pavyzdys — Morzės abėcėlė¹: — atitinka A, — — atitinka M, —. ir ... atitinka raidės N ir S. Taigi žodžio NAMAS Morzės kodas yra —. — — —. — Tai ne šifras, visi žinantys Morzės kodo lentelę gali perskaityti, ką šių taškų ir brūkšnių eilutė reiškia.

Kodavimas informatikoje naudojamas archyvuojant pradinius duomenis, kad juos būtų patogiau laikyti bei greičiau perduoti.

Dažnai naudojami kodavimo būdai, leidžiantys nustatyti, ar gautoji informacija nebuvo iškraipyta. Pavyzdžiui, jei duomenys buvo gauti iš toli, tai jie galėjo pasiekti mus su klaidomis.

Mokėdami nustatyti, ar duomenys teisingi, apsisaugosime nuo klaidingos informacijos. Kodavimas sudaro galimybę ne tik atpažinti, ar neįvyko klaidų, bet ir jas ištaisyti.

Vienas iš tokių — Golėjaus (Golay) kodas buvo naudojamas, kai kosminis laivas „Voyager“ 1979–1981 siuntė į Žemę spalvotas Jupiterio ir Saturno nuotraukas. Kiekviename 24 bitų informacijos bloke buvo galima ištaisyti iki 3 įvykusių klaidų.

Tiesą sakant kodavimas ir klaidų taisymas pasitaiko mūsų gyvenime kasdien. Juk bet kuri kalba yra puikus informacijos kodavimo būdas, sudarantis galimybę ištaisyti nemažai klaidų. Tarkime, jums paskambino draugas ir pasakė kažkokį žodį. Telefono ryšys blogas, draugo balsas girdėjosi lyg iš kokio rūšio, o gal ir jis pats linkęs taip kalbėti, lyg dudentų sau po nosim. Taigi jūs išgirdote žodį BLOKMO-TAS. Kokį žodį draugas norėjo jums pasakyti? BLOKNOTAS? O gal BEGEMOTAS? Labiau tikėtina, kad buvo iškreipta viena raidė, o ne trys. Taigi jūs dekoduojate BLOKNOTAS — pagal gautą žodį ne tik nustatėte, kad įvyko klaida, bet ją ir ištaisėte.

Kartais teisingai pavyksta dekoduoti tik tada, kai pasinaudojame konteksto teikiama in-

¹ Morzės abėcėlė pateikta, pavyzdžiui, straipsnyje: V. Stakėnas, Pusamžė teorija, *Alfa plius omega*, 1998, 2(6), 15–30.

formacija. Pavyzdžiui, jei jūs išgirdote žodį GUODAS, net ir nustatę, kad įvyko klaida, negalėsite teisingai dekoduoti. Koks žodis iš tikrųjų turėtų būti: KUODAS? NUODAS? PUODAS? JUODAS? Tačiau jeigu kontekstas buvo toks: „Koks gražus GUODAS stovi ant lentynos!“, jūs dekoduosite teisingai: PUODAS.

Brūkšninis kodas EAN

Ant prekių visi mes daug kartų matėme juodais įvairaus storio brūkšniais koduotą informaciją. Tai brūkšninis kodas EAN (*Europe Article Numeration*).

Taigi brūkšninis kodas — vertikalių juodų brūkšnelių „tvorelė“. Šiais brūkšneliais koduojama 13 skaičių, kiekvienas iš jų gali būti nuo 0 iki 9. Tie skaičiai $a_1, a_2, \dots, a_{13}$ būna parašyti po brūkšniniu kodu.

Šie skaičiai suskirstyti į tris grupes. Pirmoje grupėje yra vienas skaičius, antroje — šeši, trečioje — taip pat šeši, pavyzdžiui,

4 — 102570 — 001023.

Po kiekvienos grupės nubrėžti du siauri ilgesni juodi brūkšniai. Tarp šių skiriamųjų brūkšnių užrašyti antrosios ir trečiosios grupių skaičiai.

Antrosios grupės skaičiams $a_2, a_3, a_4, a_5, a_6, a_7$ koduoti naudojami du kodai — A ir B (1 lentelė). Koks kodas naudojamas skaičiui koduoti, priklauso nuo brūkšninio kodo pirmojo skaičiaus.

Trečiosios grupės skaičiai $a_8, a_9, a_{10}, a_{11}, a_{12}, a_{13}$ koduojami C kodu (1 lentelė).

1 lentelė

Skaičius	A kodas	B kodas	C kodas
0	0001101	0100111	1110010
1	0011001	0110011	1100110
2	0010011	0011011	1101100
3	0111101	0100001	1000010
4	0100011	0011101	1011100
5	0110001	0111001	1001110
6	0101111	0000101	1010000
7	0111011	0010001	1000100
8	0110111	0001001	1001000
9	0001011	0010111	1110100

Vienetas lentelėje reiškia vertikalų juodą brūkšnelį, nulis — baltą juostelę. Keletas paeiliui einančių vienetų ar nulių atitinka platesnį brūkšnelį ar baltą juostelę. Pastebėjime, kad kodas C gautas iš kodo A, pakeitus 0 į 1 ir 1 į 0. Kodas B gaunamas iš kodo C, užrašant C žodžius atvirkščia tvarka. Šių kodų žodžiai parinkti taip:

- visi kodų žodžiai yra skirtingi;
- visi kodo A ir kodo B žodžiai prasideda 0 ir baigiasi 1; taigi pirmos grupės skaičių kodai natūraliai atsiskiria — jie nesusilieja; nesusilieja ir antrosios grupės skaičių kodai, tik jie prasideda 1, o baigiasi 0;
- kiekvienas kodo žodis sudarytas iš poros sekų, sudarytų tik iš nulių, ir poros sekų, sudarytų iš vienetų; vadinasi, kiekvienas skaičius koduojamas dviem juodom ir dviem baltom juostelėm, tai labai suprastina dekodavimą;
- jokiame žodyje nėra daugiau kaip keturių iš eilės einančių vienetų simbolių; tai reiškia, kad vertikalūs brūkšniai gali būti ketveriopo storio: siauri, vidutiniai, platūs ir labai platūs. Todėl skaitančiajam įrenginiui nesunku apskaičiuoti, kokio storio yra vertikalūs brūkšnys. Tai nesunku padaryti ir plika akimi.

Pirmojo skaičiaus a_1 reikšmė priklauso nuo to, kuriais kodais (A ar B) koduoti kiti antrosios grupės skaičiai. Ši priklausomybė nusakyta 2 lentelėje.

2 lentelė

Skaičius a_1	Antros grupės skaičių kodai					
	a_2	a_3	a_4	a_5	a_6	a_7
0	A	A	A	A	A	A
1	A	A	B	A	B	B
2	A	A	B	B	A	B
3	A	A	B	B	B	A
4	A	B	A	A	B	B
5	A	B	B	A	A	B
6	A	B	B	B	A	A
7	A	B	A	B	A	B
8	A	B	A	B	B	A
9	A	B	B	A	B	A

Dabar aptarkime, kaip brūkšninis kodas dekoduojamas. Skaitantis įrenginys „žiūri“ į brūkšninį kodą per horizontalų plyšį statmenai kodo juostelėms. Taigi kiekviena juoda juostelė įrenginiui atrodo kaip vienokio ar kitokio ilgio linija. Iš viso jis turi pamatyti 30 tokių linijų: po dvi kiekvienam skaičiui ($12 \times 2 = 24$) ir dar po dvi kontrolines linijas po kiekvienos skaičių grupės (taigi dar $2 \times 3 = 6$).

Dekodavimo procesą galima nusakyti šitaip:

1. Perskaitomos dvi pirmosios linijos. Kadan gi jų plotis žinomas, pagal jį galima nustatyti mastelį (atstumas nuo prekės iki skaitančio įrenginio gali būti įvairus, todėl mastelį nustatyti būtina).
2. Šešis kartus skaitoma po porą juodų juostelių atsižvelgiant į tai, kokie yra atstumai tarp jų. Kiekviena juodų juostelių pora atitinka vieną kodo A arba kodo B skaičių. Šitaip perskaitomi skaičiai $a_2, a_3, \dots, a_7$. Įsimenama naudotų kodų seka.
3. Naudojantis 2 lentelė pagal skaičiams $a_2, \dots, a_7$ koduoti kodų A ir B seką nustatomas skaičius a_1 .
4. Praleidžiamos dvi siauros juostelės, skiriančios antrąją ir trečiąją skaičių grupes.
5. Šešis kartus perskaitoma po porą juodų juostelių atsižvelgiant į jų tarpusavio nuotolį. Šitaip nustatomi skaičiai $a_8, a_9, \dots, a_{13}$.
6. Perskaitytus visus brūkšninio kodo skaičius, tikrinama, ar nebuvo klaidų. Randama suma $S = a_1 + 3a_2 + \dots + 3a_{12} + a_{13}$ ir tikrinama, ar skaičius S dalijasi iš 10. Jeigu nesidalija, vadinasi, nuskaityta klaidingai ir skaitoma iš naujo.

Perskaitykite kokios nors prekės brūkšninį kodą. Kadan gi po brūkšniniu kodu surašyti skaičiai, galėsite patikrinti, ar nesuklydote.

Ar brūkšniniais kodais galima pasikliauti?

Taigi bet kurios prekės EAN brūkšninis kodas yra trylikos skaičių $a_1, a_2, \dots, a_{12}, a_{13}$ rinkinys. Pirmieji du skaičiai koduoja prekės gamintojo šalį, kiti skaičiai — kitą su preke susijusią informaciją, o paskutinis skaičius a_{13} yra kontrolinis. Jis parenkamas taip, kad suma

$S = a_1 + 3a_2 + \dots + 3a_{12} + a_{13}$
dalytųsi iš 10.

Jeigu skaitant kodą įvyko viena klaida, t.y. vienas skaičius perskaitytas klaidingai, tai suma S jau nebesidalys iš 10 ir bus galima padaryti išvadą, kad nuskaityta klaidingai.

O jeigu įvyks dvi klaidos? Kokia tikimybė, kad galėsime pastebėti, jog kodas perskaitytas klaidingai?

Tarkime, kad taip ir įvyko: neteisingai perskaitytas k -asis ir m -asis skaičiai. Turėjo būti a_k ir a_m , o perskaityta e_k ir e_m . Taigi

$$a_k \neq e_k, \quad a_m \neq e_m, \quad k \neq m.$$

Nesunku suskaičiuoti, kiek yra skirtingų porų k, m . Jų yra štai tiek: $A_{13}^2 = 13 \cdot 12 = 156$. Tikrinant, ar įvyko klaidų, naudojama tik suma S , todėl svarbu žinoti, kokie koeficientai šioje sumoje parašyti prieš a_k ir a_m . Nesunku pastebėti:

- 1) jei $k + m$ yra lyginis skaičius, tai koeficientai vienodi (lygūs 1 arba 3);
- 2) jei $k + m$ yra nelyginis skaičius, tai koeficientai skirtingi (vienas yra lygus 1, kitas — 3);

Pirmąjį atvejį atitinka $A_6^2 + A_7^2 = 78$ poros, antrąjį — $156 - 78 = 78$ poros, taigi abu atvejus galime laikyti pasitaikančiais su tomis pat tikimybėmis. Kai klaidingai nuskaityti skaičiai, kurių numerių suma lyginė, tai įvykusios klaidos bus nepastebėtos, jei

$$e_k + e_m \equiv a_k + a_m \pmod{10} \quad \text{arba}$$

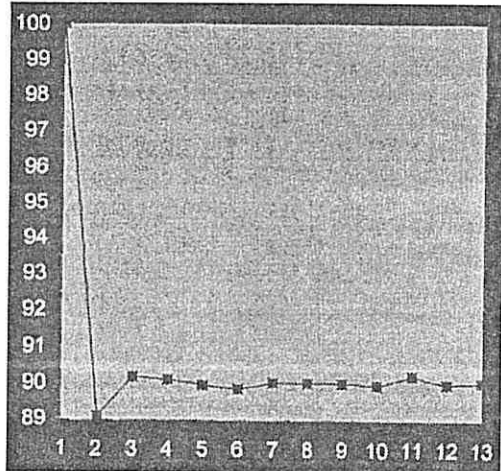
$$3e_k + 3e_m \equiv 3a_k + 3a_m \pmod{10}.$$

Kaip dažnai tai gali pasitaikyti? Jei k ir m fiksuosime, tai skirtingų ketvertų a_k, a_m, e_k, e_m su sąlyga

$$a_k \neq e_k, \quad a_m \neq e_m, \quad k \neq m$$

bus lygiai 8100. Kiek yra atvejų, kai teisinga $e_k + e_m \equiv a_k + a_m \pmod{10}$, t.y. klaida neaptinkama? Galima išspręsti šį nesudėtingą kombinatorikos uždavinį arba reikalingą skaičių apskaičiuoti kompiuteriu. Gausime 900 atvejų. Taigi tikimybė, kad bus pastebėta skaitymo klaida, jei neteisingai perskaityti k -asis ir m -asis skaičiai, kai $k + m$ yra lyginis, lygi

$$1 - \frac{900}{8100} \approx 0,889.$$



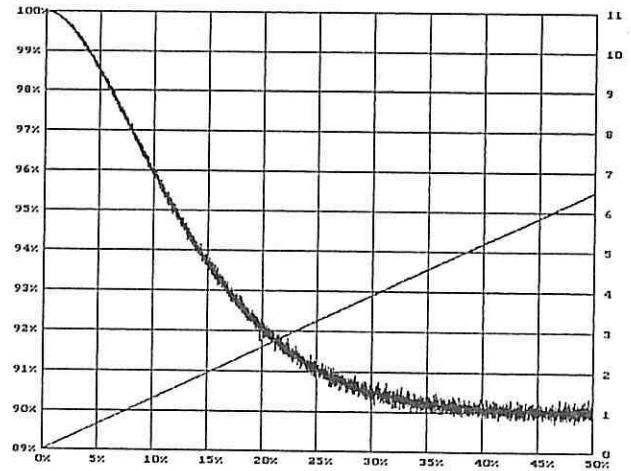
1 pav.

Tą patį rezultatą gauname ir tuo atveju, kai $k + m$ yra nelyginis.

Vadinasi, galime padaryti tokią išvadą: jei neteisingai perskaityti du kodo skaičiai, tai tikimybė, kad bus pastebėtos skaitymo klaidos, lygi 0,889. Ar tai daug, ar mažai? Pasvarstykime. Tarkime, norime apgauti skaitymo įrenginį, t. y. norime, kad jis pripažintų neteisingą kodą. Teisingame kode pakeitus du skaičius, tai mums pasiseks su tikimybe 0,111. O dabar parašykime bet kokią trylikos skaičių rinkinį ir duokime įrenginiui perskaityti. Kontrolinė suma S gali su vienodomis tikimybėmis dalytis iš 10, dalybos liekana gali būti lygi 1 ir kt. Įrenginys neatpažins apgaulės, jei S dalysis iš 10. Taigi tikimybė, kad visai atsitiktinis skaičių rinkinys bus pripažintas kaip geras kodas, lygi 0,1. Ji nedaug skiriasi nuo tikimybės dviejų klaidų atveju. Kartojant bandymą, tarkime, 1000 kartų, galima tikėtis, kad keičiant du gero kodo skaitmenis pavyks apgauti aparatą maždaug 111 kartų, o naudojant visai atsitiktinius skaičių rinkinius — maždaug 100 kartų.

Tikimybė (procentais), kad klaidos bus pastebėtos, kai jų įvyko 1, 2, ..., 13, parodyta 1 paveiksle.

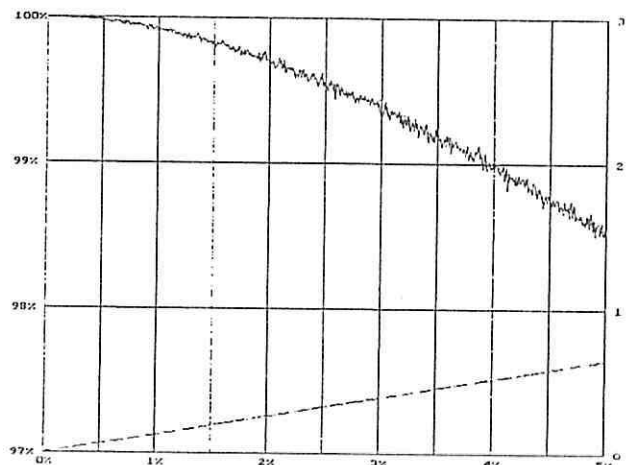
O dabar tarkime, kad skaitantis įrenginys vieną skaičių klaidingai perskaito su tikimybe p . Vadinasi, skaitydamas visą trylikos skaičių kodą jis gali jį perskaityti teisingai arba padaryti nuo 1 iki 13 klaidų. Kokia tikimybė, kad naudojamas sumą S įrenginys aptiks klaidą?



2 pav.

Atlikto modeliavimo rezultatai pavaizduoti 2 paveiksle. Vieno simbolio iškraipymo tikimybė buvo keičiama nuo 0 iki 0,5 (nuo 0% iki 50%) žingsniu 0,0001. Kiekvienai tikimybės reikšmei buvo atliekama 100 000 bandymų. Taigi grafikas nubrėžtas atlikus 500 milijonų bandymų. Pirmojoje vertikalioje ašyje atidėta klaidos aptikimo tikimybė, ji gauta skaičių atveju, kai klaida buvo aptikta, padalijus iš 100 000. Tiesi linija rodo vidutinį vieno bandymo klaidų skaičių, kuris gautas bendrą klaidų skaičių padalijus iš 100 000.

Padidinę šio grafiko dalį, atitinkančią mažas vieno skaičiaus neteisingo skaitymo tikimybes, gausime vaizdą, pavaizduotą 3 paveiksle.

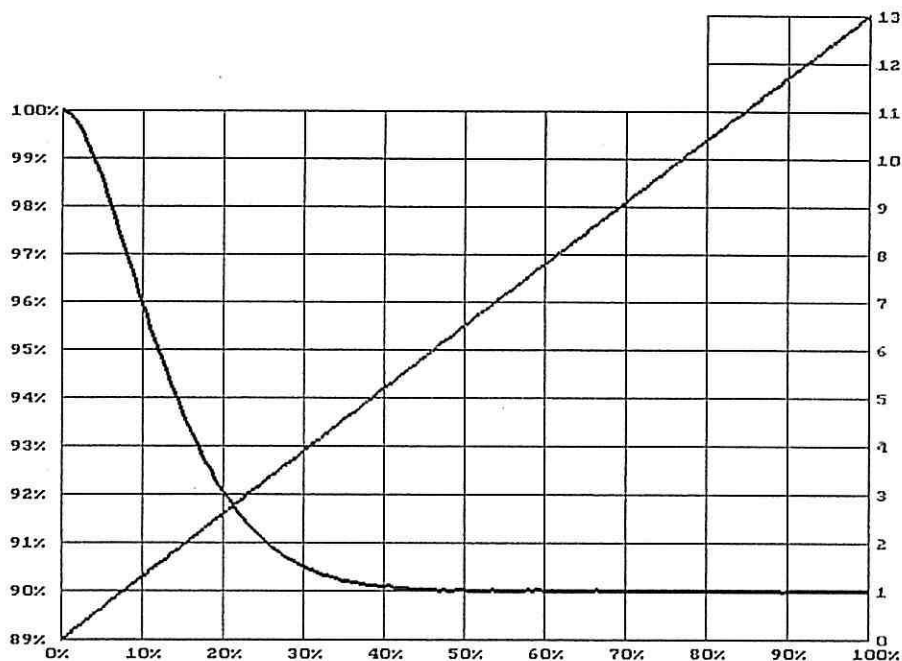


3 pav.

O čia vieno skaičiaus neteisingo nuskaitymo tikimybę keitėme nuo 0 iki 1 žingsniu, lygiu 0,005, kiekvienai tikimybės reikšmei atlikdami 10 000 000 bandymų. Taigi iš viso atlikta

2 milijardai skaičiavimų (4 pav.).

Atkreipkime dėmesį, kad jei simbolio iškraipymo tikimybė didesnė už 0,5, klaidų aptikimo tikimybė jau nebesikeičia.



4 pav.