

Seznam projektov

1. V prvi domači nalogi smo se spraševali kako Vam bo ta predmet koristil pri Vašem študiju (oziroma delu). Razmislimo malo bolj natančno o **matematiki** (njenem smislu, prenosu znanja/učenju, itd.). Ozrmo se naokoli in pogledjmo kaj znajo na to temo povedati drugi, npr. Charles Darwin:

“Matematik je slepec v mračni sobi, ki išče črno mačko, ki je ni tam”.

- [Mag] Z. Magajna, Je mogoče učiti matematiko, *Obzornik mat. fiz.* **43** (1996) 6, str. 183-193.
[Vid1] I. Vidav, Razmišljanja o matematiki, *Obzornik mat. fiz.* **36** (1989), str. 65-79.
[Dra] Z. Šporer, Oh, ta matematika, *Presek* **11/5,6**.
[Wig] E. P. Wigner (prev. S. Oblak), Vloga matematike v naravoslovju, *Obzornik mat. fiz.* **8** (1961), str. 145.
[Bez] D. Bezek, Od števil h geometriji, umetnosti in igri, *Presek* **6/4**, str. 196-202.
[Puc] I. Pucelj, Inverzori, *Presek* **9/3**, str. 138-140.
[Baj] K. Bajc, Vsakdanje in vendarle imenitno, *Presek* **10/1**, str. 16-18.
[Gut] I. Gutman (prev. B. Mohar), Matematične živalice, *Presek* **12/1**, str. 34-42.

2. Nahajamo se na pragu vsesplošnega komuniciranja in elektronskega trgovanja na Internetu. Preko Interneta so dostopne številne podatkovne baze in z vsakim dnem bolj občutimo vpliv na šolstvo, znanost ter družbo v širšem pomenu. Mnoge družbe se pripravljajo ponuditi usluge in blago na mrežah. Varnost in zaščita bosta poglobitni komponenti razvoja elektronskega trgovanja. Osrednji cilj pa bo razviti enotne metode, protokole in usluge za varno okolje in s tem elektronsko trgovanje.

Z razvojem telekomunikacij in procesiranja informacij so se povečale zahteve po večji varnosti pri prenosu informacij, po zagotovitvi nespremenjenih informacij in tudi zahteve po razjasnitvi, kdo je pooblastil/avtoriziral določene dele informacij.

Kriptografija je veda, ki nam ponuja konkretne rešitve za pravkar omenjena področja in probleme ter s tem predstavlja osnovo informacijske družbe. Na vseh področjih komunikacij nastajajo standardi za kriptografsko zaščito. Kriptografija javnih ključev predstavlja nenadomestljivo orodje za poenostavitev upravljanja ključev in realizacijo varne komunikacije. Predstavi eno shemo javnih ključev.

- [Zu] J. Zupan, Nekaj o kriptografskih metodah, *Obzornik mat. fiz.*, **25** (1978), 129-136.
[Ma] B. Magajna, O tajnopisih, *Obzornik mat. fiz.*, **38** (1991), 9-18.
[Ven3] M. Vencelj, To in ono o tajnopisih, *Presek* **22**, str. 257-263.
[Ven4] M. Vencelj, Šifriranje z javnim ključem, *Presek* **22**, str. 354-357.
[JT] A. Jurišić, A. Trojar, Pametna kartice, *Uporabna informatika*, **5/1** (1997), 37-45.

3. **Števila** nas spremljajo skozi tisočletja, vendar pa niso bila vedno enaka (glej tudi [Bez] v točki 1 in [Str1] v točki 8).

- [JZ] B. Jurčič-Zlobec, Števila skozi tisočletja, *Presek* **3**, str. 103-113.
[Sku] T. Skubic, Dvojiški številski sistem, *Presek* **3**, str. 98-102, 172-176.
[Špo] Z. Šporer, Oh, ta matematika, *Presek* **11/5,6**.
[Vid4] I. Vidav, Racionalna in iracionalna števila, *Obzornik mat. fiz.* **9** (1962), str. 1-6.

4. **Deljivost števil in kongruence.** Naj bosta a in b celi števili in m naravno število. Potem relacijo $m \mid b - a$ (m deli $b - a$, oziroma razlika $b - a$ je deljiva s številom m) pogosto raje zapišemo v naslednji obliki

$$a \equiv b \pmod{m}$$

in rečemo, da je število a kongruentno številu b po modulu m , oziroma števili a in b dasta isti ostanek pri deljenju s številom m (kongruenca = ujemanje, skladnost). Prouči osnovne lastnosti kongruenc in njihovo uporabno.

[Lav5] B. Lavrič, Ogrevjmo se za kongruence, *Presek* **15/4**, str. 193.

[For4] F. Forstnerič, O kongruencah, *Presek* **7/3**, str. 145-152.

[Pag] D. Pagon, Kongruence in Eulerjev izrek, *Presek* **15/4**, str. 194-196.

5. **Matematična indukcija** je močno sredstvo za dokazovanje matematičnih izrekov. Mi smo si ogledali le nekaj primerov. Poišči čim več različnih primerov uporabe.

[Pri2] N. Prijatelj, O matematični indukciji, *Presek* **5/2**, str. 77-80.

[Mil1] D. M. Milošević (prev. P. Petek), Vsota kubov, *Presek* **10**, str. 115-117.

[Mas] M. Mastnak (prir. D. Felda), Vsota n -tih potenc prvih m števil, *Presek* **19**, str. 331-333.

[Ven1] M. Vencelj, 100 let Peanovih aksiomov, *Presek* **19**, str. 108-110.

[Tu] A. Turnšek, Vsota potenc naravnih števil, *Presek* **14**, str. 48-52.

6. **Absolutna vrednost** lahko precej skrajša zapis kakšne zveze ocene ali zakona in zato nanjo pogosto naletimo. Tako moramo znati reševati/obravnavati tudi (ne)enačbe ali pa izraze v katerih nastopa absolutna vrednost.

[Haf] I. Hafner, Reševanje enačb in neenačb v katerih nastopa absolutna vrednost, *Presek* **12/4**, str. 201-203.

7. Računanje s **približki** je neizbežno, zato moramo znati najti čim boljše približke in ocenjevati napake do katerih pride pri računanju z njimi. Pri tem si lahko pomagamo z diferencialom, Taylerjevo vrsto, pa tudi z integrali.

[Pet1] P. Petek, O pravokotnih trikotnikih in o približkih za koren iz dva, *Presek* **2/1**, str. 26-28.

[Dom2] V. Domajnko, Babilonski približek za $\sqrt{2}$, *Presek* **21**, str. 40-45.

[Pet2] P. Petek, Kako spravimo ulomek v škatlo, *Presek* **3**, str. 163-165.

[Pet3] P. Petek, Deseti koren iz deset, *Presek* **9**, str. 200-202.

[Pet4] P. Petek, Kako se je godilo številu π , *Presek* **3**, str. 139-143, 193-196.

[Av] F. Avsec, Iracionalnost števila π , *Obzornik mat. fiz.* **3** (1956), str. 117-118.

[Kra1] E. Kramar, Ocenjevanje pribliška števila π na osnovi preproste statistične metode, *Presek* **12/4**, str. 196-200.

[Vid5] I. Vidav, O številu π , *Obzornik mat. fiz.* **2** (1955), str. 73.

[Vid6] I. Vidav, Število π na deset tisoč decimalk, *Obzornik mat. fiz.* **6** (1959), str. 77.

8. **Kvadratna enačba** nekoč in danes ter razcepi polinomov.

[Str1] M. Strnad, Kvadratna enačba pri Babiloncih, *Presek* **16**, str. 271-273.

[Str2] J. Strnad, Zakaj so antene parabolične, *Presek* **16**, str. 334-337.

[Dom1] V. Domajnko, Descartesova geometrijska metoda za reševanje kvadratnih enačba, *Presek* **18**, str. 66-69.

[And] V. Andrić (prev. M. Pintar), Razcepi polinomov pri reševanju nalog o številih, *Presek* **13/3**, str. 129-134.

9. Pascalov trikotnik in binomski obrazec.

[For2] F. Forstnerič, Pascalov trikotnik, *Presek* **8/4**, str. 200-205.

[Pav] G. Pavlič, Pascal, Fibonacci in božično drevo, *Presek* **22**, str. 129-132, IX.

10. Kotne funkcije, število e in kompleksna števila.

[Kob] D. Kobal, Kotne funkcije, *Presek* **15**, str. 56-60.

[Leg1] P. Legiša, Pravilo 72 in število e , *Presek* **20**, str. 290-293.

[For3] F. Forstnerič, Kompleksna števila, *Presek* **15**, str. 98-103.

[Raz3] M. in N. Razpet, Kvadratno kolo, verižica in traktrisa, *Presek* **25**, str. 294-299.

11. O realnih zaporedjih, konvergenca in vrstah, ki jih dobimo iz aritmetičnega in geometrijskega zaporedja.

[Pri4] N. Prijatelj, O realnih številih, *Obzornik mat. fiz.* **16/2** (1969), str. 49-55.

[Tom] G. Tomšič, O konvergenca, *Obzornik mat. fiz.* **10** (1963), str. 111-115.

[Ced] A. Cedilnik, Geometrijska in harmonična vrsta, *Presek* **23**, str. 40-45.

12. Fibonaccijevo zaporedje. Najpomembnejše delo iz algebre srednjega veka je razprava Liber abaci (Knjiga o abaku). Napisal jo je znani italjanski matematik Leonardo Pizano (Pisano, Leonardo iz Pizze), bolj poznan pod imenom Fibonacci (Fibonacci, skrajšano filius Bonacci, kar pomeni Bonaccijev sin). Prvič je bilo izdano leta 1202, predelano pa leta 1228. V njem je bilo obdelano skoraj vse kar so takrat vedeli o aritmetiki in algebi. Odigralo je pomembno vlogo v razvoju zahodnoevropske matematike v nekaj naslednjih stoletjih. S tem delom so v evropsko matematično misel prenešena mnoga znanja arabskih matematikov, med njimi tudi desetiški sistem.

Dober del te knjige sestavljajo naloge. Med njimi je tudi naslednja naloga:

Par zajcev, začeni od svojega drugega meseca življenja naprej, enkrat na mesec prinese na svet po en par mladičev. Če smo imeli na začetku leta en par zajcev, koliko jih bo na koncu leta?

Naj bo $f(n)$ število parov zajcev po n -tem mesecu. Očitno je $f(0) = 1$, $f(1) = 2$. Po izteku $(n + 2)$ -tega meseca bomo imeli $f(n + 1)$ starih parov in prav toliko novorojenih parov, kolikor smo jih imeli na koncu n -tega meseca, tj. $f(n)$. Torej zadovoljujejo členi zaporedja $\{f(n)\}$ naslednjo relacijo:

$$f(n + 2) = f(n + 1) + f(n).$$

Iz te relacije izračunamo zaporedoma

$$\begin{aligned} f(2) &= f(1) + f(0) = 2 + 1 = 3, \\ f(3) &= f(2) + f(1) = 3 + 2 = 5, \\ f(4) &= f(3) + f(2) = 5 + 3 = 8. \dots \end{aligned}$$

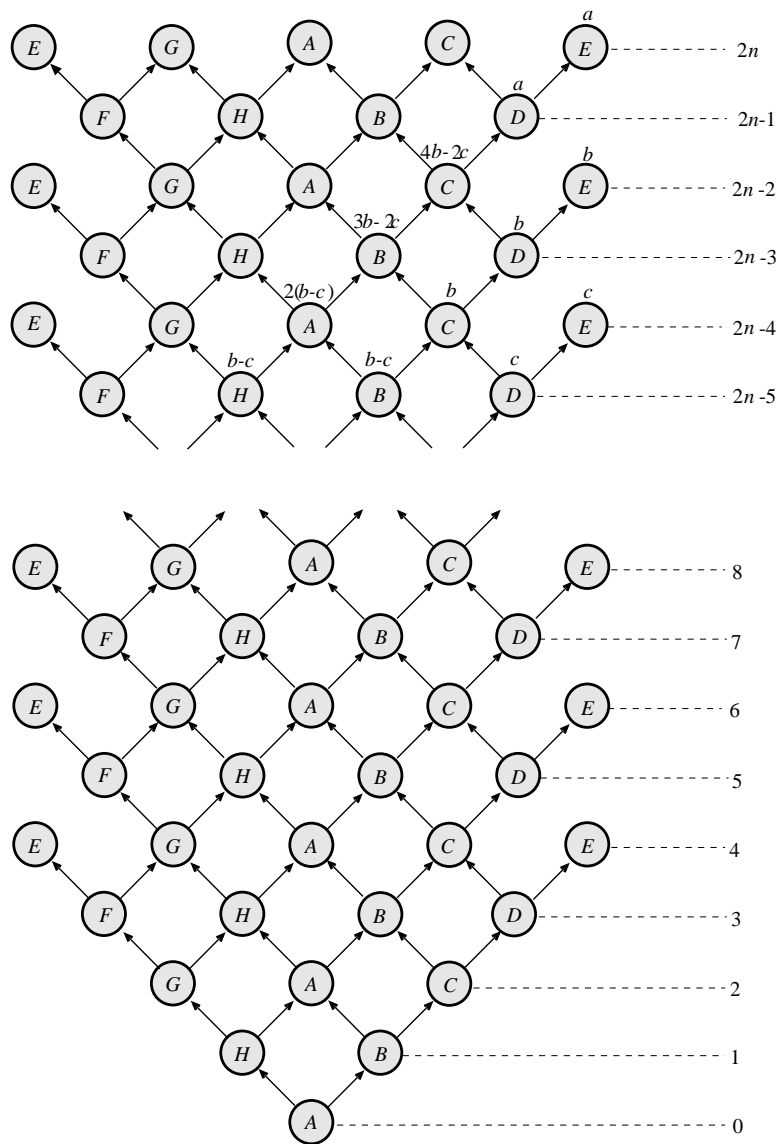
Tako dobimo po tem postopku, da je iskano število zajcev enako $f(12) = 377$. Obstaja pa tudi eksplicitna formula za n -ti člen tega zaporedja. Pravzaprav znamo rešiti splošno diferenčno enačbo oblike

$$x_{n+2} = px_{n+1} + qx_n,$$

s pomočjo geometrijskih zaporedij, kjer sta p in q poljubni celi števili.

Olimpijska naloga z žabo (Velika Britanija 1979): Naj bosta A in E nasprotni oglišči pravilnega osemkotnika. V oglišču A je žaba, v oglišču E pa žabec. Z vsakega oglišča osemkotnika lahko žaba skoči le na sosednje oglišče. Izjema je le oglišče E , na katerem žaba obstane. Naj bo a_n število načinov, v katerih pride žaba z oglišča A na oglišče E po natančno n skokih. Dokaži, da velja za $n = 1, 2, \dots$,

(a) $a_{2n-1} = 0$, (b) $a_{2n} = \frac{x^{n-1} - y^{n-1}}{\sqrt{2}}$, kjer je $x = 2 + \sqrt{2}$ in $y = 2 - \sqrt{2}$.



Slika: Iz mreže skokov žabe dobimo rekurzivno enačbo $a_{2n} = 4a_{2n-2} - 2a_{2n-4}$, ki jo nato rešimo kot splošno diferencialno enačbo, kot v primeru Fibonaccijevega zaporedja.

[BL] E. Beloglavec in M. Lakner, Fibonaccijevo zaporedje, *Presek* **14**/4, str. 216-219.
 [Juv1] M. Juvan, Posplošena Fibonaccijeva zaporedja, *Presek* **14**, str. 150-152.
 [JK] M. Juvan in K. Kokalovič, Še enkrat o Fibonaccijevih zaporedjih, *Presek* **14**, str. 334-337.
 [Kra2] E. Kramar, Diferenčne enačbe v elementarni geometriji, *Presek* **16**/3, str. 274-280.
 [Spa] J. Šparovec, Fibonaccijeva števila in zlati rez, *Matematika v šoli* **VI**/1,2, str. 101-105.
 [Jur] A. Jurišič, Rešene naloge z mednarodnih matematičnih olimpiad, 1. del, 1978-88, *Knjižnica Sigma* **46**, DMFA Slovenije, Ljubljana 1989.

13. Odvodi, ekstremi in posredne funkcije.

[Pri1] N. Prijatelj, Nekaj preprostih ekstremov, *Presek* **3**, str. 3-8.

[Zal] B. Zalar, Odvod polinomov in njegova uporaba, *Presek* **21**, str. 336-338.

[Vad] A. Vadnal, Konstrukcija posredne funkcije, *Obzornik mat. fiz.* **14** (1967), str. 78-79.

14. Teorija grafov in njena uporaba na drugih področjih.

[Vra] J. Vrabec, *Obzornik mat. fiz.* **14** (1967), str. 58, 10.

[Re] D. Repovš, Problem o barvanju kart, *Presek* **5**, str. 73-76.

[Pis1] T. Pisanski, Najcenejše drevo, *Presek* **7**, str. 226-237.

[Pis2] T. Pisanski, Problem štirih barv, *Presek* **9**, str. 68-70.

[Gut] I. Gutman (prev. B. Mohar), Teorija grafov in kemija, *Presek* **9/1**, str. 3-13.

[Bat1] V. Batagelj, Hamiltonova naloga za grafe, *Presek* **11/1**, str. 4-16.

[Pis3] D. Bajc, T. Pisanski, Najnujnejše o grafih, *Presek* **12/6**.

[Dob] M. Dobovišek, Eulerjeva formula za ravninske grafe, *Presek* **19**, str. 98-100.

[Ven2] M. Vencelj, Eulerjeva poliederska formula, *Presek* **19**, str. 2-6.

15. Cauchyjeva neenakost in neenakosti med potenčnimi sredinami (npr. aritmetična sredina je večja ali enaka geometrijski sredini istih števil) sta najbolj znani neenakosti in jih pogosto uporabljamo na vseh koncih matematike in drugih vedah.

[Drn1] R. Drnovšek, Cauchyjeva neenakost, *Presek* **15**, str. 355-357.

[Mil3] D. M. Milošević (prev. B. Lavrič), Sredini na tehtnici, *Presek* **16/4**, str. 194-196.

16. Integral in njegova uporaba (glej tudi referenco [Vid6] v točki 6).

[Vid2] I. Vidav, O definiciji določenega integrala, *Obzornik mat. fiz.* **8** (1961), str. 49-54.

[Lav1] B. Lavrič, Prostornina paraboloida, *Presek* **16**, str. 4-7.

[Lav2] B. Lavrič, Izmerimo svitek, *Presek* **19**, str. 66-71.

17. Vektorji - vir pomembnih matematičnih pojmov. Z njimi lahko poenostavimo mnoge dokaze, lahko pa jih uporabimo tudi za definicijo trigonometričnih funkcij.

[Vid3] I. Vidav, Vektorji - vir pomembnih matematičnih pojmov, *Obzornik mat. fiz.* **6** (1959), str. 1-10.

[Pri3] N. Prijatelj, Vektorji v elementarni geometriji, *Obzornik mat. fiz.* **10** (1963), str. 97-110.

[Lav3] B. Lavrič, Paralelogramsko pravilo, *Presek* **20**, str. 146-150.

18. Pitagorov izrek je en izmed najstarejših izrekov, in zanj imamo na voljo mnoge dokaze, lahko pa ga tudi posplošimo.

[Pi] J. Piškur, Pitagorjev izrek čigav si?, *Presek* **5**, str. 9-10.

[Rih] L. Rihtar, Pitagorjev izrek, *Presek* **6**, str. 69-70.

[Puc] I. Pucelj, Posplošitev Pitagorjevega izreka, *Presek* **7**, str. 9-10.

[Lav4] B. Lavrič, Paralelogramsko pravilo, *Presek* **20**, str. 146-150.

[Raz] M. Razpet, Pitagorov izrek iz trapeza, *Presek* **25**, str. 7.

19. Matrike niso samo skladišča informacij, ki nam pomagajo pri delu z vektorji. Zanimiva je tudi motivacija za definicijo množenja matrik, motivacija za definicijo determinante, itd.

[Su] A. Suhadolc, Matrike kot posplošitev pojma števila I, II, *Presek* **25**, str. 2-7 in 104-111.

[Pa] S. Pahor, Kaj imata skupnega zaporedje zasukov kartezičnega sistema v ravnini in zaporedje leč na optični klopi? - I, *Obzornik mat. fiz.* **37** (1990), str. 11-16.

[Arn] O. Arnuš, Matrike - ali skladišča informacij, *Presek* **23**, str. 65-69.

20. Permutacije, verjetnost in statistika.

[Kla] S. Klavžar, O igri 15 in permutacijah, *Presek* **16**, str. 159-163.

[Vad] A. Vadnal, O definicijah matematične verjetnosti, *Obzornik mat. fiz.* **4** (1957), str. 97-104.

[Vid7] I. Vidav, Teorija števil in verjetnostni račun, *Presek* **21**, str. 264-271.

[Moh] B. Mohar, O posojilih, *Presek* **13/1**, str. 20-23.

[Bat2] V. Batagelj, Sandokan, *Presek* **5/3**, str. 131-133.

21. Algebrائي enačbi s celimi koeficienti pri kateri nas zanimajo samo celoštevilčne rešitve pravimo **diofantska enačba**. Linearne diofanske enačbe znamo rešiti v splošnem z več kot dva tisoč let starim Evklidovim algoritmom. Spomnimo se, da pri Evklidovem algoritmu za računanje največjega skupnega delitelja $D(a, b)$ števil a in b najprej delimo a z b , oziroma poiščemo natanko določeni števili s in r za kateri velja

$$a = bs + r, \quad 0 \leq r < |b|.$$

Če je ostanek r enak 0, potem je $D(a, b) = b$, sicer pa delimo zadnji delitelj z zadnjim ostankom (katerega lahko izberemo tako, da je njegova absolutna vrednost ne presega vrednosti $|b|/2$) in to ponavljamo vse dokler ne pridemo do ostanka 0 (to se mora zgoditi, saj se absolutne vrednosti ostankov neprestano zmanjšujejo). Potem je zadnji od nič različen ostanek največji skupni delitelj števil a in b . Ta proces lahko predstavimo z naslednjimi enačbami

$$\begin{aligned} a &= s_1 b + r_1, & |r_1| < |b| \\ b &= s_2 r_1 + r_2, & |r_2| < |r_1| \\ r_1 &= s_3 r_2 + r_3, & |r_3| < |r_2| \\ &\vdots \\ r_{k-3} &= s_{k-1} r_{k-2} + r_{k-1}, & |r_{k-1}| < |r_{k-2}| \\ r_{k-2} &= s_k r_{k-1} + r_k, & |r_k| < |r_{k-1}| \\ r_{k-1} &= s_{k+1} r_k + 0. \end{aligned}$$

Potem je $D(a, b) = r_k$. Ta algoritem pa lahko uporabljamo tudi za amproksimacijo realnih števil z racionalnimi števili.

[Kri] F. Križanič, Diofantske enačbe, *Presek* **5/3**, str. 134-141.

[Gra1] J. Grasselli, Diofantske enačbe, *Knjižnica Sigma* **38**, DMFA Slovenije, Ljubljana 1984.

[Gra2] J. Grasselli, Diofantski približki, *Knjižnica Sigma* **51**, DMFA Slovenije, Ljubljana 1992.

[Vid9] I. Vidav, Teorija števil in elementarna geometrija/izbor člankov, *Knjižnica Sigma* **62**, DMFA Slovenije, Ljubljana 1996.

[Leg2] P. Legiša, Verižni ulomki, *Presek* **10/1**, str. 216-212.

22. **Iterativne metode** uporabljamo za reševanje enačb, ki jih ne znamo rešiti direktno.

[Pah3] S. Pahor, Reševanje enačb z iteracijo, *Obzornik mat. fiz.* **6** (1959), str. 74-77.

[For1] F. Forstnerič, Metoda zaporednih približkov, *Presek* **8/2**, str. 81-92.

[Dom2] V. Domažnjko, Babilonski približek za $\sqrt{2}$, *Presek* **21**, str. 40-45.

[Drn2] R. Drnovšek, Računanje približkov kvadratnega korena iz naravnega števila, *Presek* **24**, str. 372-375.

23. **Grupe, homomorfizmi in faktorske grupe.**

[Vid8] I. Vidav, Vloga grup v elementarni matematiki, *Obzornik mat. fiz.* **16/1** (1969), str. 1-4.

Paul R. Halmos

“Mathematics is not a deductive science – that’s a cliché. When you try to prove a theorem, you don’t just list the hypotheses, and then start to reason. What you do is trial and error, experimentation, guesswork.”

I Want to be a Mathematician, Washington: MAA Spectrum, 1985.

Paul R. Halmos

“...the source of all great mathematics is the special case, the concrete example. It is frequent in mathematics that every instance of a concept of seemingly great generality is in essence the same as a small and concrete special case.”

I Want to be a Mathematician, Washington: MAA Spectrum, 1985.

???

“ Sometimes a research is a lot of hard work in looking for the easy way.”

David Hilbert (1900)

“The art of doing mathematics consists in finding that special case which contains all the germs of generality.”

David Hilbert (1900)

“Every definite mathematical problem must necessarily be susceptible of an exact settlement, either in the form of an actual answer to the question asked, or by the proof of the impossibility of its solution and therewith the necessary failure of all attempts... // However unapproachable these problems may seem to us and however helpless we stand before them, we have nevertheless, the firm conviction that their solution must follow by a finite number of purely logical processes... // “We hear within us the perpetual call: There is the problem. Seek its solution. You can find it by pure reason...” .”

Hermann Weyl (1885 - 1955)

“We are not very pleased when we are forced to accept a mathematical truth by virtue of a complicated chain of formal conclusions and computations, which we traverse blindly, link by link, feeling our way by touch. We want first an overview of the aim and of the road; we want to understand the idea of the proof, the deeper context.”

Unterrichtsblltter fr Mathematik und Naturwissenschaften, 38, 177-188 (1932).

Hermann Weyl (1885 - 1955)

“My work has always tried to unite the true with the beautiful and when I had to choose one or the other, I usually chose the beautiful.”

In an obituary by Freeman J. Dyson in Nature, March 10, 1956.

Alfred North Whitehead (1861 - 1947)

“Fundamental progress has to do with the reinterpretation of basic ideas.”

W.H. Auden and L. Kronenberger The Viking Book of Aphorisms, New York: Viking Press, 1966.

Alfred North Whitehead (1861 - 1947)

“We think in generalities, but we live in details.”

W.H. Auden and L. Kronenberger The Viking Book of Aphorisms, New York: Viking Press, 1966.

Alfred North Whitehead (1861 - 1947)

“Apart from blunt truth, our lives sink decadently amid the perfume of hints and suggestions.”

W.H. Auden and L. Kronenberger The Viking Book of Aphorisms, New York: Viking Press, 1966.

Norbert Wiener (1894-1964)

“Progress imposes not only new possibilities for the future but new restrictions.”

The Human Use of Human Beings.

Norbert Wiener (1894-1964)

“The Advantage is that mathematics is a field in which one’s blunders tend to show very clearly and can be corrected or erased with a stroke of the pencil. It is a field which has often been compared with chess, but differs from the latter in that it is only one’s best moments that count and not one’s worst. A single inattention may lose a chess game, whereas a single successful approach to a problem, among many which have been relegated to the wastebasket, will make a mathematician’s reputation.”

Ex-Prodigy: My Childhood and Youth.

Malcom X

“I’m sorry to say that the subject I most disliked was mathematics. I have thought about it. I think the reason was that mathematics leaves no room for argument. If you made a mistake, that was all there was to it.”

Mascot.