

Veliki jezični modeli – potraga za umjetnom inteligencijom (2. dio)¹

RENI BANOV²

Pojavom velikih jezičnih modela nesumnjivo svjedočimo jednoj od najznačajnijih revolucija u povijesti znanosti i tehnologije, možda na razini otkrića tiskarskog stroja ili uspostave međumrežja. Njihova sve učestalija primjena na problemima za koje ponekad i nisu pripremljeni upućuje na oprez i pažnju prilikom uporabe alata za rad s jezičnim modelima. U ovom dijelu prikaza jezičnih modela ilustrirat ćemo kako njihova primjena u nastavi matematike može djelomično biti korisna za studente i nastavnike u domeni rješavanja (i zadavanja) primjera i zadataka tijekom obrazovnog procesa i donekle od pomoći u istraživačkom radu. Razvojem velikih jezičnih modela nastavnicima se nudi pogodnost relativno brze i jednostavne izrade primjera zadataka temeljem kojih studenti mogu dublje razumjeti obrađeni nastavni sadržaj. Pored toga, pomoću dostupnih alata za jezične modele studentima i nastavnicima omogućena je suradnja s virtualnim asistentom, prilagođena njihovim potrebama i razini usvojenog znanja. Ovdje je nužno istaknuti kako su veliki jezični modeli samo strojevi za formiranje blokova teksta (rečenica, paragrafa, cijelih dokumenata...) u dotičnom jeziku, ali nisu provjereni znalci (eksperti) za područja na kojima se pomoću njih generira sadržaj. Nastavnici odnosno svi korisnici velikih jezičnih modela trebaju kritički pristupiti generiranim rezultatima, drugim riječima, nipošto ih prigrliti kao istinite bez prethodne provjere njihove vjerodostojnosti. Neovisno o tomu što se pomoću jezičnih modela mogu jednostavno generirati sadržaji iz brojnih područja, u matematici takvi alati ne mogu zamijeniti interakciju studenta s nastavnikom koja je nužna za potpuno razumijevanje matematičkih pojmova. U ovom nastavku prikazat ćemo kako se pomoću ChatGPT alata (besplatna razina modela 5.1) za primjenu jezičnog modela može izraditi esej na hrvatskom jeziku za zadanu temu iz matematike. Napominjemo kako u ovom članku koristimo navedeni alat, ali ne pre-judiciramo njegovu superiornost ili nedostatke u odnosu na druge alate za primjenu jezičnih modela. Štoviše, slični rezultati na temu pisanja matematičkog eseja mogu se postići primjenom ostalih trenutno raspoloživih alata (Gemini, Claude, Grok, Llama, DeepSeek, ...) od kojih su brojni dostupni u besplatnoj varijanti, a u novije se vrijeme

¹Prvi dio članka objavljen je u Poučku broj 102

²Reni Banov, Tehničko veleučilište u Zagrebu

pojavljaju i jezični modeli razvijeni u sustavu otvorenog koda (eng. *open source LLM models*), također prikladni za ovakvu primjenu. Valja napomenuti da LLM modeli iz otvorenog koda često podržavaju samo engleski jezik za upite i rezultate, pa tako omogućuju pisanje eseja i drugih tekstova isključivo na tom jeziku.

Može li LLM napisati matematički esej?

Odgovor na to pitanje nesumnjivo je potvrđan: veliki jezični modeli mogu pripremiti matematički esej na odgovarajući upit. Međutim, matematički esej dobiven pomoću alata za jezične modele treba promatrati u kontekstu akademske čestitosti i vjerodostojnosti korištenih činjenica, pa ćemo u ovom radu nastojati prikazati upravo taj kontekst njihove uporabe. Ističemo kako to nisu jedini konteksti u kojima se može valorizirati primjena jezičnih modela u obrazovnom procesu, te da su brojni i drugi važni aspekti primjene, posebice u akademskoj zajednici [1,2]. Stoga nikako ne treba shvatiti ovaj članak kao preporuku za pisanje matematičkog eseja ili drugih tekstova pomoću jezičnih modela, štoviše smatramo kako je izvornost rada nezaobilazni kriterij u akademskoj (i u drugim) zajednici. Akademska zajednica nije prostor za izradu znanstvenih i stručnih replika, već treba poticati u svom radu izvornost i istinitost kao neizostavne smjernice (ograde) u individualnom razvoju pojedinca.

Promotrimo na Slici 1. kako ChatGPT alat „razumije” pojam matematičkog eseja.

poznaš li pojam matematičkog eseja

Da — **matematički esej** je oblik pisanog rada koji spaja matematički sadržaj s esejističkim stilom izlaganja. Za razliku od klasičnih matematičkih zadataka ili dokaza, matematički esej naglasak stavlja na:

Što je matematički esej?

Matematički esej je tekst u kojem se:

- **objašnjava**, istražuje ili **promišlja** neki matematički koncept,
- matematičke ideje iznose **jasno, logično i argumentirano**, ali u narativnom ili refleksivnom stilu,
- često se uključuje **motivacija**, povijesni kontekst, primjene ili osobno razumijevanje teme.

Karakteristike matematičkog eseja

- **Preciznost** matematičkog jezika, ali bez nužne formalnosti dokaza.
- **Povezivanje matematike s pričom**, kontekstom ili problemom.
- **Objašnjava procesa razmišljanja**, a ne samo rješenja.
- Može uključivati formule, grafove, primjere — ali samo kao podršku narativu.
- Cilj je učiniti matematičku ideju **razumljivom i smislenom** čitatelju.

Slika 1. Pojam matematičkog eseja iz ChatGPT-ja

Dobiveni odgovor razumljivo i koncizno opisuje pojam matematičkog eseja pa se moramo zapitati odakle tako dobar opis.

odakle su definicije sadržaja matematičkog eseja

Definicije i opis sadržaja matematičkog eseja koje sam ti dao temelje se na kombinaciji:

1. **Akademskih i obrazovnih izvora** – mnoge škole i sveučilišta definiraju matematički esej kao pisani rad koji istražuje matematičku temu na argumentiran i razumljiv način, a ne samo formalno rješavanje zadataka. Primjeri uključuju vodiče za pisanje matematičkih eseja na sveučilištima poput MIT-a, Cambridgea ili Stanforda.
2. **Pedagoške literature i priručnika za nastavnike** – knjige i članci o metodama poučavanja matematike često spominju da esej omogućuje učenicima da:
 - istraže i reflektiraju matematičke koncepte,
 - povežu matematiku s stvarnim životom ili poviješću,
 - razvijaju sposobnost argumentacije i komunikacije matematičkih ideja.
3. **Struktura i praksa pisanja matematičkih eseja** – definicija i karakteristike koje sam naveo temelje se i na uobičajenim preporukama za matematičke eseje u nastavi: preciznost, primjeri, motivacija, objašnjenje procesa razmišljanja i povezivanje s realnim problemima.

Drugim riječima, nisam citirao jedan specifičan izvor, već sam sažeo opće pedagoške smjernice i akademske definicije koje se koriste za pojam „matematički esej“ u obrazovanju i matematičkoj komunikaciji.

Hrvatski izvori / vodiči i radovi o matematičkom esej

Izvor / rad	Opis / što nudi	Napomena o izvornosti (hrvatski / adaptacija)
Hrvatsko matematičko društvo (HMD) — rad <i>Esej iz matematike kao metoda vrednovanja matematičke komunikacije</i>	Analiza ideje i koncepta matematičkog eseja u nastavi, razmatranje vrednovanja „matematičke komunikacije“, prijedlog kriterija vrednovanja eseja, primjeri upotrebe u školskom kontekstu. Hrčak	Originalno — rad je objavljen na hrvatskom jeziku.
Poučak (časopis HMD-a) — rad <i>Esej iz matematike</i> (ili poglavlje u njemu)**	Diskutira uvođenje eseja u nastavu matematike, predlaže kako bi takav format zadatka trebao izgledati, definira što se traži od učenika: tekst, objašnjenja, matematičko razmišljanje, moguće skice, primjere, modeliranje... Hrčak	Originalno na hrvatskom i primjenjiv u našem obrazovnom sustavu.
Rad objavljen u zborniku skupa nastavnika — <i>Esej iz matematike</i> (autori: Azra Stašćik, Amanda Glavaš)	U radu su dane teme pogodnih za eseje, smjernice, kriteriji ocjenjivanja i primjer jednog učenikova eseja (iz strojarske škole, na temu stereometrije) — dakle konkretan "model" matematičkog eseja. CroRIS	Originalno, napisano na hrvatskom, prilagođeno školskom kontekstu.

Slika 2. Izvori ChatGPT-ju za pojam matematičkog eseja

Iz odgovora (Slika 2.) vidljivo je kako su primarni izvori za pojam matematičkog eseja na hrvatskom jeziku nastali u okvirima aktivnosti Hrvatskog matematičkog društva, što nam daje određenu sigurnost za vjerodostojnost opisa dobivenog iz alata. Ostali izvori koji ovdje nisu navedeni prilagođeni su iz prijevoda ili su inspirirani tekstovima s engleskog govornog područja. Ohrabreni uvjerljivim objašnjenjem pojma matematičkog eseja možemo uz pomoć ChatGPT jezičnog modela pokušati napisati esej o Pépinovu testu za prostost Fermatovih brojeva.

Pisanje eseja o Pépinovu testu prostosti LLM alatom

Sredinom 17. stoljeća (oko 1640.) francuski matematičar Pierre de Fermat (1601. – 1665.) postavio je slutnju (koja je kasnije opovrgnuta) kako su svi brojevi oblika

$$F_m = 2^{2^m} + 1, \quad m = 0, 1, 2, \dots$$

prosti, pa se njemu u čast takvi brojevi nazivaju *Fermatovim* brojevima. Ako je zaista neki Fermatov broj prost, tada se on naziva *Fermatov prosti broj*. Nakon manje od jednog stoljeća (oko 1732.) veliki švicarski matematičar Leonhard Euler (1707. – 1783.) pokazao je da već F_5 nije prost broj, štoviše, Euler je uspješno našao njegovu faktorizaciju

$$F_5 = 4294967297 = 641 \cdot 6700417$$

te je na taj način kontraprimjerom dokazao kako Fermatova slutnja nije točna. Međutim, pitanje prostosti ostalih Fermatovih brojeva još je uvijek ostalo otvoreno i nakon Eulerova kontraprimjera. Krajem 19. stoljeća (oko 1877.) drugi francuski matematičar Théophile Pépin (1826. – 1904.) u svom radu [3] predložio je jednostavan ali računski zahtjevan test [4] za provjeru prostosti Fermatovih brojeva, koji u modernom zapisu glasi

$$F_m \text{ prost} \Leftrightarrow 3^{(F_m-1)/2} \equiv -1 \pmod{F_m}, \quad m \geq 1.$$

Pépin je izvorno za test koristio bazu 5 kod modularnog potenciranja za $m > 1$, dok je bazu 3 predložio također francuski matematičar Francois Proth (1852. – 1879.) otprilike godinu dana kasnije [5]. Uzimajući u obzir navedene povijesne činjenice, pokušajmo pomoću ChatGPT alata sastaviti ogledni matematički esej na temu Pépinova testa.

Kontekst za pisanje eseja

Postavljanje konteksta za odabranu temu predstavlja možda najvažniji korak u primjeni alata za jezične modele. Naime, kako je opisano u prvom dijelu [6] prikaza jezičnih modela, kontekst je ključan parametar u određivanju pozornosti za pojmove koji se pojavljuju u komunikaciji s jezičnim modelom. Za ovaj primjer matematičkog eseja postaviti ćemo kontekst Fermatovih brojeva, dok će konkretan pojam biti Pépinov test.

Možeš li složiti matematički esej o Pepinovom testu u kontekstu Fermatovih brojeva?

Naravno — evo koherentnog, matematički usmjerenog eseja o Pepinovom testu i njegovoj ulozi u ispitivanju prostosti Fermatovih brojeva.

Pepinov test u kontekstu Fermatovih brojeva

1. Uvod

Fermatovi brojevi čine jednu od najzanimljivijih klasa prirodnih brojeva u teoriji brojeva. Definisani su izrazom

$$F_n = 2^{2^n} + 1,$$

oni rastu izuzetno brzo i pokazuju impresivnu strukturalnu regularnost. Pierre de Fermat je pretpostavio da su svi brojevi oblika F_n prosti. Iako su prva četiri (F_0 do F_4) doista prosti, kasnije se pokazalo da je Fermatova pretpostavka pogrešna.

Ključnu ulogu u tom otkriću odigrao je **Pepinov test**, izuzetno elegantan i efikasan kriterij prostosti specifično konstruisan za Fermatove brojeve.

Slika 3. Postavljanje konteksta komunikacije s jezičnim modelom

Nakon kratkog „razmišljanja” (nekoliko sekundi) ChatGPT prezentira svoj odgovor na upit za izradu matematičkog eseja. Zanimarimo *nehrvatske* jezične konstrukcije te se fokusirajmo na vjerodostojnost činjenica u napisanome eseju. Uočimo na Slici 4. kako je ChatGPT za definiciju i povijesni okvir ponudio modernu definiciju testa koja sugerira da je Pépin u izvorniku koristio bazu 3 kod modularnog potenciranja iako znamo kako je ta baza naknadno predložena u Prothovu radu.

3. Pepinov test — definicija i istorijski kontekst

Test je 1877. godine formulisao Théophile Pépin.

On kaže:

Fermatov broj $F_n = 2^{2^n} + 1$ je prost ako i samo ako

$$3^{(F_n-1)/2} \equiv -1 \pmod{F_n}.$$

Drugim riječima:

- Ako je kongruencija zadovoljena, Fermatov broj je prost.
- Ako nije, broj je složen.

Pepinov test (za razliku od većine testova prostosti) daje **potpunu ekvivalenciju** — nema mogućnosti lažno pozitivnih ili negativnih rezultata.

Slika 4. Definicija Pépinova testa iz ChatGPT-ja

Kako bismo potvrdili sumnju da ChatGPT model za originalnu formulaciju Pépinova testa u eseju predlaže verziju koja je nastala nešto kasnije, provjerit ćemo „razumijevanje” pojma baze za njegov jezični model.

Netočnost povijesnog navoda za bazu u Pépinovu testu

U Pépinovu testu za Fermatove brojeve F_m indeksa većeg od jedan, bazu 3 možemo zamijeniti bilo kojim prirodnim brojem b za koji je Jacobijev simbol ([7]) jednak -1 . Naime, vrijedi sljedeća generalizacija Pépinova testa:

Teorem (generalizacija Pépinova testa) [8]

Za Fermatove brojeve F_m ($m > 1$) i prirodne brojeve $b > 1$ ekvivalentne su sljedeće tvrdnje:

1. F_m je prost i vrijedi $\left(\frac{b}{F_m}\right) = -1$
2. $b^{(F_m-1)/2} \equiv -1 \pmod{F_m}$

Budući da je ChatGPT model nastao obradom velikog broja stranica s međumrežja, pretpostavljamo da bi model morao imati zapisane informacije o popisu dostupivih baza za Pépinov test. Jedan od izvora dostupivih baza je OEIS [9] kolekcija (enciklopedija) cjelobrojnih nizova brojeva za različite namjene. Niz poznat pod

oznakom A129802 upravo predstavlja popis (ne svih) baza koje se mogu koristiti u testu uz neka ograničenja. Ponajprije, provjerimo putem ChatGPT-ja nužnost korištenja baze 3 za Pépinov test.

Da li je nužno koristiti bazu 3 ili mogu biti i druge baze?

Kratak odgovor: nije nužno koristiti baš bazu 3, ali je baza 3 jedina poznata jednostavna univerzalna baza za Pépinov test. Druge baze *mogu* raditi, ali moraju ispuniti vrlo specifične uslove — i te uslove nije jednostavno provjeriti unaprijed.

Evo detaljnog objašnjenja.

Slika 5. Nužnost baze 3 u Pépinovu testu

Nakon toga provjerimo poznaje li model OEIS enciklopediju nizova brojeva unutar koje se nalazi izračunati niz A129802 za baze u Pépinovu testu. Uvedimo OEIS enciklopediju (Slika 6.) u kontekst za određivanje pozornosti pojmova iz eseja.

Da li poznáš OEIS biblioteku nizova cijelih brojeva?

Da — poznajem OEIS (Online Encyclopedia of Integer Sequences).

To je najveća i najpoznatija online biblioteka nizova cijelih brojeva, koju je započeo Neil Sloane još 1964. godine. Danas sadrži preko 360.000 nizova, uz detaljne informacije za svaki:

- definicije i formule,
- generirajuće funkcije,
- programi (Mathematica, PARI/GP, Maple, Python...),
- bibliografske reference,
- veze s drugim nizovima,
- matematička svojstva,
- primjene u kombinatorici, teoriji brojeva, algoritmima...

Slika 6. Online enciklopedija cjelobrojnih nizova (OEIS)

Mogu li se brojevi iz niza A129802 koristiti za bazu u Pépin testu?

Misao za 15s >

Kratko: da — brojevi iz niza A129802 su upravo kandidati koji se mogu koristiti kao baze za (generalizirani) Pépinov test. OEIS opis tog niza kao „possible bases for Pépin primality test for Fermat numbers”. [OEIS +1](#)

Par važnih pojašnjenja:

- Pépinov test u svojoj standardnoj formi koristi bazu 3. Generalizacija traži bazu a takvu da za svaki prost Fermatov broj F_n imamo

$$a^{(F_n-1)/2} \equiv -1 \pmod{F_n}.$$

Slika 7. OEIS niz A129802 izvor i kriterij za odabir baze u Pépinovu testu

Model ispravno prepoznaje brojeve iz OEIS niza A129802 (Slika 7.) te daje objašnjenje kriterija za brojeve koji se mogu koristiti za bazu u generaliziranom Pépinovu testu. Međutim, na eksplicitni upit (Slika 8.) je li Pépin u izvornom obliku testa koristio bazu 5, dobijemo autoritativan, ali pogrešan odgovor za koji model nudi dva pogrešna zaključka (Slika 9.) o korištenju baze 3 i 5 u povijesnom i standardnom Pépinovu testu.

Zar nije Pepin koristio broj 5 za bazu?

Ne — Pépin nije koristio 5 kao bazu. Pépinova izvorna formulacija iz 1877. godine koristi *baš bazu 3*.

To je klasični, standardni i jedini povijesno ispravan oblik testa:

$$F_n = 2^{2^n} + 1 \text{ je prost} \iff 3^{(F_n-1)/2} \equiv -1 \pmod{F_n}.$$

Dakle:

- Originalni Pepinov test → baza 3.
- Baza 5 nije dio povijesnog testa.

Slika 8. Pitanje baze u izvornom Pépinovu radu

Zaključak

- ✓ Povijesni i standardni Pepinov test koristi isključivo bazu 3.
- ✓ Broj 5 je ponekad prihvatljiva baza u nekim modernim generalizacijama, ali to nije Pepinov originalni test.
- ✓ OEIS A129802 sadrži brojeve koji su „moguće baze“ u generalizacijama, ali ne odnosi se na izvornu Pépinovu formulaciju.

Slika 9. Zaključak o bazi u izvornom obliku Pépinova testa

Detaljnije pojašnjenje (Slika 10.) daje odgovore zašto je model ponudio pogrešne zaključke o izvornom radu.

U originalnoj literaturi nalazim da je Pepin koristio broj 5 za bazu a bazu 3 je nešto kasnije predložio Francois Proth. Možeš mi pojasniti o čemu se radi?

Da — dobro si primijetio — tvoja informacija je tačna i istorija je malo složenija nego što često prikazuju pojednostavljeni izvori. Evo objašnjenja „tko je šta prvi“ i zašto se ponekad nalazi tvrdnja da je Théophile Pépin koristio bazu 5, a ne 3, a da je baza 3 došla kasnije putem François Proth (i drugih).

✓ Šta kažu izvori: Pépin je u originalu koristio 5

- Prema izvoru koji sažima historiju, Pépin je u svom originalnom radu 1877. predložio test s bazom 5 (ili alternativno 10). Matematička Fa... +2
- U radu „17 Lectures on Fermat Numbers” navodi se da „u svom zapisu iz 1877. Pépin je koristio bazu 5 umjesto 3” i da je, prema njegovim riječima, kao baza mogla poslužiti i 10. Vdoc +1
- Stranica posvećena testu (npr. Prime-Glossary) kaže da 3 može biti zamijenjena „bilo kojim pozitivnim k za koji je Jacobi simbol $(k|F_n) = -1$ ”, i da to uključuje npr. 5 i 10. PrimePages +1

Dakle: u originalnoj formulaciji Pépin — barem prema historijskim izvorima — kao baza nije nužno bila 3, nego 5 (ili 10).

Slika 10. Pojašnjenje za baze 3 i 5 u Pépinovu izvornom radu

Pojašnjenje je naravno samouvjereno, ali ipak u zadnjoj rečenici dopušta mogućnost da Pépin u izvornom radu koristi bazu 5 te da je pokazao kako se baza 10 također može koristiti za njegov test prostosti Fermatovih brojeva. Na ukazanu pogrešku (Slika 11.) vidimo da je ChatGPT model korigirao činjenice o bazi za Pépinov test te možemo očekivati kako će ispravljena verzija zaključka biti uključena u esej.

Znači tvoja tvrdnja "Povijesni i standardni Pepinov test koristi isključivo bazu 3." je pogrešna?

Razmišljao 4 sekunde/i >

Da — bila je pogreška u mojoj ranijoj formulaciji. Ispričavam se zbog netočnosti — hvala što si ukazao na to.

Ispravak i pojašnjenje (kratko)

- **Pépin (1877)** je u svojem originalnom radu formulirao test koristeći **bazu 5** (spominjao je i 10 kao alternativu).
- **Proth** je ubrzo nakon toga (1878) primijetio/ predložio **bazu 3** za isti tip testa.
- **Édouard Lucas** i drugi kasnije su formalizirali i dokazali općenitiji oblik koji objašnjava zašto bilo koja baza a s $\left(\frac{a}{F_n}\right) = -1$ daje ekvivalentni kriterij — pa se u modernoj literaturi često navodi *Pépinov test u obliku s bazom 3*.

Dakle: moja tvrdnja „Pépinov test koristi isključivo bazu 3” bila je netočna u povijesnom smislu. Ispravno je reći da **Pépinov original** koristi 5 (ili 10), dok je **moderni standardni oblik** često zapisan s bazom 3 zahvaljujući Prothu/Lucasu i kasnijim interpretacijama.

Slika 11. Priznanje i ispravak pogreške

Pojam „univerzalne baze“ za Pépinov test

U dosadašnjoj konverzaciji model je koristio pojam univerzalne baze za Pépinov test, pa pokušajmo pomoću ChatGPT modela razjasniti što znači pojam „univerzal-

na baza” za ovaj test te postoje li neke druge univerzalne baze za Pépinov test, primjerice baza 5 (Slika 12.) ili neka druga.

Mogu li onda zaključiti da je 5 također univerzalna baza ako ju je Pépin koristio?

Kratak odgovor: **Ne**, iz toga što je Pépin koristio 5 u originalu *ne slijedi* da je 5 univerzalna baza. Čak i ako ju je on upotrijebio, to *nije* matematički dokaz univerzalnosti.

Evo jasnog objašnjenja.

1. Šta znači „univerzalna baza“?

Baza a je *univerzalna* za Pépinov test ako za **svaki** prosti Fermatov broj

$$F_n = 2^{2^n} + 1,$$

vrijedi ekvivalencija:

$$F_n \text{ prost} \iff a^{(F_n-1)/2} \equiv -1 \pmod{F_n}.$$

Za univerzalnost treba dokazati da:

1. Ako je F_n prost, tada a ima maksimalni mogući red,
2. Odnosno da je

$$\left(\frac{a}{F_n}\right) = -1 \text{ za svaki prosti } F_n.$$

Dakle, univerzalnost je vrlo **stroga**, **jaka tvrdnja**. ↓

Slika 12. Objašnjenje pojma univerzalne baze

Iz interpretacije pojma *univerzalna baza* za ChatGPT model u ovom kontekstu zaključujemo kako model interpretira taj pojam za Pépinov test kao onaj broj $b > 1$ za koji će vrijediti jednakost

$$b^{(F_m-1)/2} \equiv -1 \pmod{F_m}$$

za **sve Fermatove proste** brojeve te „smatra” kako jedino broj 3 ispunjava tu jednakost. Međutim, ta jednakost vrijedi za provjeru prostosti svih Fermatovih brojeva F_m ($m \geq 1$), ali ne vrijedi za provjeru Fermatova broja $F_0 = 3$. Za Fermatove brojeve F_m ($m \geq 1$), možemo, naravno, naći brojne druge univerzalne baze, primjerice oblika $3 \cdot 2^n$, gdje je n paran prirodan broj. Pokušajmo navesti ChatGPT na otkrivanje univerzalnih baza upravo toga oblika (Slika 13.).

Jesu li onda višekratnici oblika 3 puta potencije broja 2 univerzalne baze? Naprimjer, brojevi 6, 12, 24, 48, ...

Misao za 20s >

Dobar i pravično precizan upit — zahvaljujem. Kratki odgovor:

Da — među brojevima oblika $3 \cdot 2^k$ upravo oni s k parnim (tj. $3 \cdot 4$, $3 \cdot 16$, $3 \cdot 64$, ...) zadovoljavaju uvjet koji čini bazu „univerzalnom” za Pépinov tip testa (kod Fermatovih brojeva F_n s $n \geq 1$).

Objašnjenje slijedi.

1. Uvjet za „univerzalnu“ bazu a je (ekvivalentno) da za svaki prosti Fermatov broj $p = F_n$ vrijedi

$$\left(\frac{a}{p}\right) = -1,$$

tj. a je kvadratni *nekvadratni* ostatak modulo svakog prostog F_n . U grupi $(\mathbb{Z}/p\mathbb{Z})^\times$ (koja je ciklička reda 2^{2^n}) to osigurava da a ima maksimalni red i daje Pepinovu ekvivalenciju

$$a^{(p-1)/2} \equiv -1 \pmod{p}.$$

3. Dakle:

- Za sve Fermatove proste $p = F_n$ s $n \geq 2$ faktor 2^k ne mijenja simbol (jer $(2|p) = 1$), pa ponašanje ovisi samo o $(3|p) = -1$.
- Da bi pokrili i slučaj $p = 5$ (tj. F_1), potrebno je da k bude paran.
Zaključak: $3 \cdot 2^k$ je univerzalna baza (u smislu Pepinove ekvivalencije za sve proste Fermatove brojeve F_n s uobičajenom konvencijom $n \geq 1$) upravo kada je k paran.

Slika 13. Druge univerzalne baze za test

Uz to smo dobili točno objašnjenje kada će baza biti univerzalna u Pépinovu testu, pa podsjetimo ChatGPT (Slika 14.) kako je prije samo nekoliko upita tvrdio da je samo broj 3 univerzalna baza.

Dakle postoji više univerzalnih baza za Pepinov test, a ponovno si me zavarao tvrdnjom "Do danas je samo baza 3 poznata kao univerzalno ispravna i dokazana."

Razumijem potpuno zašto ti je nastala konfuzija — termin „univerzalna baza“ često se koristi neformalno i tada stvara krivi dojam da postoji nekakav dokazani beskonačni skup baza koje *uvijek* rade za Pépinov test. Hajdemo razjasniti stvar do kraja i vrlo precizno.

Što je stvarno dokazano, a što nije?

1. Zašto baza 3 „radi“ za sve Fermatove brojeve

Može se dokazati (na temelju svojstava Fermatovih brojeva i kvadratnih ostataka) da je:

$$3^{(F_n-1)/2} \equiv -1 \pmod{F_n}$$

nužan i dovoljan uvjet da je F_n prost.

To znači: 3 je dokazano univerzalna baza.

Slika 14. Objašnjenje zašto je 3 „dokazano“ univerzalna baza

Uočimo kako je u odgovoru ispuštena tvrdnja da navedeni uvjet prostosti vrijedi za sve Fermatove brojeve s indeksom većim od 0, ali za te Fermatove brojeve ta jednakost vrijedi i za baze oblika $3 \cdot 2^n$ kada je n paran prirodan broj, upravo činjenica koju je ChatGPT dokazao u objašnjenju za prethodni upit. Dokažimo pomoću ChatGPT-

ja modificiranu tvrdnju da u Pépinovu testu za $m > 1$ možemo koristiti baze oblika $3 \cdot 2^n$ kada je n bilo koji prirodan broj. Početak dokaza za tu tvrdnju je na Slici 15. koja je ujedno i primjer korištenja LaTeX naredbi za postavljanje upita.

Možeš li dokazati da vrijedi $(2b)^{(F_m-1)/2} \equiv b^{(F_m-1)/2} \pmod{F_m}$ za $m > 1$ i za $b \geq 0$ za baze u Pepin testu?

Misao za 17s >

Da — to se lako dokaže korištenjem Eulerova kriterija / Legendreovog simbola. Pokazat ću precizno i kratko.

Neka $m > 1$ i neka $p := F_m = 2^{2^m} + 1$. Pretpostavimo da je $b \geq 0$ takav da je b prihvatljiva baza za Pépinov test za p , tj. $\gcd(b, p) = 1$ (ako je $b \equiv 0 \pmod{p}$ tvrdnja je trivijalno istinita jer su obje strane $\equiv 0$). Trebamo pokazati

$$(2b)^{(p-1)/2} \equiv b^{(p-1)/2} \pmod{p}.$$

Razložimo:

$$(2b)^{(p-1)/2} = 2^{(p-1)/2} b^{(p-1)/2}.$$

Dakle dovoljno je pokazati da

$$2^{(p-1)/2} \equiv 1 \pmod{p}.$$

Slika 15. Početak dokaza tvrdnje

Dokazanu ćemo tvrdnju uključiti u esej, kao i činjenicu da su baze 5 i baze oblika $3 \cdot 2^n$ također univerzalne za Fermatove brojeve s indeksom većim od 1.

Možemo li zaključiti da su baze 3,6,12,24,48,... univerzalne za $m > 1$?

Misao za 9s >

Da — za sve Fermatove proste brojeve $p = F_m$ s $m > 1$ svaki broj oblika $a = 3 \cdot 2^k$ zadovoljava Pépinovu ekvivalenciju

$$a^{(p-1)/2} \equiv -1 \pmod{p}.$$

Evo kraćeg, jasnog dokaza.

Možeš li sada nadopuniti prethodni esej s tom činjenicom

Naravno — u nastavku je proširena i ispravljena verzija eseja o Pépinovu testu, sada uključujući i klasu univerzalnih baza oblika $3 \cdot 2^k$ za sve Fermatove proste brojeve s $m > 1$.
(Tekst je samostalna, zaokružena cjelina.)

Da li je povijesna baza 5 univerzalna za $m > 1$?

Da — baza 5 jest univerzalna za sve Fermatove proste brojeve s $m > 1$.
Ispod je kratko, potpuno rigorozno obrazloženje.

Slika 16. Univerzalne baze za Fermatove brojeve za $m > 1$

Dodajmo još činjenicu da samo prva dva Fermatova prosta broja mogu biti baze za test (Slika 17.)

Mogu li Fermatovi brojevi biti baze za Pepin test?

Zanimljivo pitanje! Odgovor je **da**, ali **samo trivijalno i uz vrlo ograničene uvjete**. Objasnit ću detaljno.

Znači samo Fermatovi brojevi 3 i 5 su korisne baze u Pepin testu za $m > 15$

Da — ako govorimo strogo o Fermatovim brojevima kao bazama, tada je slika sljedeća:

✓ **1. $F_0 = 3$**

Baza 3 je poznata univerzalna baza za Pépinov test:

$$3^{(F_m-1)/2} \equiv -1 \pmod{F_m} \quad \text{za sve } m > 0.$$

Dakle, 3 radi za cijeli niz Fermatovih brojeva.

✓ **2. $F_1 = 5$**

Baza 5 daje Pépinovu kongruenciju za $m > 1$.

Slika 17. Fermatovi brojevi za bazu u Pépinovu testu

te zatražimo izradu konačne verzije eseja koju možemo preuzeti iz ChatGPT alata u različitim popularnim formatima (docx, pdf,...). Na Slici 18. prikazana je skraćena verzija eseja koja uključuje uvodni paragraf, te sažetak i zaključak o Pépinovu testu prostosti za Fermatove brojeve.

možeš to dodati u konačnu verziju eseja

Pepins Test Esej
Kopiraj Uredi Preuzmi

Pépinov test u kontekstu Fermatovih brojeva – proširena i konačna verzija

1. Uvod

Fermatovi brojevi definirani su kao:

$$F_m = 2^{2^m} + 1, \quad m \geq 0.$$

Pierre de Fermat je pretpostavio da su svi brojevi ovog oblika prosti, no već je Euler 1732. pokazao da je F_5 složen. Danas je poznato da su prosti samo prvi Fermatovi brojevi: F_0, F_1, F_2, F_3, F_4 .

Najjači poznati test prostosti specifičan za Fermatove brojeve jest Pépinov test, koji daje potrebni i dovoljni uvjet za prostost svakog Fermatovog broja F_m s $m > 0$.

8. Konačni sažetak

✓ Univerzalne baze za Pépinov test:

- 3 (univerzalna za sve $m > 0$),
- 5 (univerzalna za sve $m > 1$),
- sve baze oblika $3 \cdot 2^k$ (univerzalne za $m > 1$).

✗ Fermatovi brojevi kao baze:

- 3 i 5 rade,
- svi ostali Fermatovi brojevi ne mogu dati Pépinovu kongruenciju.

9. Zaključak

Pépinov test je izuzetno elegantan jer omogućuje testiranje prostosti specifične klase brojeva korištenjem samo jedne modularne ekspanencijacije. Razumijevanje koje baze su univerzalne zahtijeva analizu kvadratnih ostataka modulo Fermatovih brojeva, što vodi do neočekivanog, ali jednostavnog zaključka:

Najkorisnije i univerzalne baze za Pépinov test su 3 i 5 i svi brojevi oblika $3 \cdot 2^k$, dok ostali Fermatovi brojevi ne mogu služiti kao baze.

Slika 18. Uvod, sažetak i zaključak eseja

Na ovom jednostavnom primjeru izrade matematičkog eseja o Pépinovu testu prostosti za Fermatove brojeve ilustrirano je nekoliko bitnih primjedbi na uporabu jezičnih modela u području matematike te posljedično u drugim znanostima i tehnicima gdje je matematika nezamjenjiv alat. Korisnik mora moći dobiti točne činjenice iz jezičnog modela jer, kao što smo na jednostavnom primjeru vidjeli, ChatGPT autoritativno prezentira činjenice koje nisu bile povijesno utemeljene niti činjenično precizne za matematički tekst. Poznato je da jezični modeli kreativno povezuju nepovezive pojmove ili pojmove iz različitih ne koreliranih okvira za različita područja [11], pa je iznimno važno prilikom njihove uporabe obratiti pozornost na činjeničnu točnost teksta. Druga bitna primjedba na uporabu jezičnih modela sadržana je u činjenici kako tekst pripremljen pomoću jezičnog modela više ne predstavlja samostalan rad. U brojnim znanstvenim i tehničkim okruženjima takvi tekstovi mogu dovesti do povećanja plagijarizma² na intelektualnoj ili tehnološkoj razini. Usko vezano za prethodno navedeno je i primjedba na generički stil pisanja tekstova. Prihvaćajući u potpunosti takve gotove ponuđene tekstove, gubi se inovativnost i individualnost intelektualnog izričaja pojedinca, što umanjuje vrijednost rada. Tu treba istaknuti kako su svjetski poznati jezici (po svojoj zastupljenosti) u prednosti spram manje zastupljenih jezika, primjerice, veći izvor građe na engleskom jeziku čini generičke tekstove teže prepoznatljivim kao takve u odnosu na generičke tekstove na hrvat-

²plagijat (njem. Plagiat < franc. plagiat, prema lat. plagiūm: otimanje, krađa), slijepo oponašanje, odn. prisvajanje tuđega djela, u cjelini ili u pojedinim odlomcima. Marcijal je prvi upotrijebio za knjiž. kradljivca izraz plagiarius. Hrvatska enciklopedija, mrežno izdanje. Leksikografski zavod Miroslav Krleža, 2013. – 2025. <https://enciklopedija.hr/clanak/plagijat> (9. 12. 2025.)

skom jeziku. Daljnja primjedba na uporabu jezičnih modela odnosi se i na pitanje kompetentnosti i savjesnosti pri pisanju radova, odnosno na pitanje treba li se autor doista osloniti na ChatGPT ili neki drugi alat za pisanje. Drugim riječima, ako autor posjeduje znanje o tematici koju želi razraditi, izložiti i sl., zar mu je doista potreban takav alat koji ga „po mnogim kriterijima” prividno može nadmašiti?

LLM i matematika

Za kraj se možemo zapitati o odnosu matematike i umjetne inteligencije apstrahirane u obliku velikih jezičnih modela. O matematici se često razmišlja kao o apstraktnom polju lišenom svake emotivne veze s kompleksnim osobnim životnim iskustvima. Često u nastavi matematike čujemo pitanja oblika „Što će mi to trebati u životu?” i „Zašto to učimo?” Istina je, međutim, sasvim suprotna. Matematika je usko isprepletena s našim doživljajem stvarnosti; od početaka razvoja civilizacije pa sve do današnjih dana matematika je bila i još uvijek jest alat kojim se služimo kako bismo percipirali svijet oko nas. Bitna je značajka što matematika također predstavlja jezik koji nam omogućuje međusobnu razmjenu novog znanja, kao i postojećeg znanja preuzetog iz djela velikih znanstvenika koji su živjeli prije nas. U tom smislu, matematika nije samo polje za studiranje, već je sastavni dio nas i naše svijesti koju nije poželjno zamijeniti umjetnom slikom.

Literatura:

1. Y. Huang, J. Wilson, *Evaluating LLM-Based Automated Essay Scoring: Accuracy, Fairness, and Validity*, Proceedings of the Artificial Intelligence in Measurement and Education Conference (AIME-Con) – Volume 2: Works in Progress, 2025; 71 - 83
2. I. Rizos, N. Gkrekas, *The impact of LLMs on mathematics education and research at the university*, Social Sciences & Humanities Open, Vol. 12, 2025., doi:10.1016/j.ssa-ho.2025.101969
3. P. Pépin, *Sur la formule $2^{2^n} + 1$* , C.R. Acad. Sci. Paris 85 (1877.), 329 - 331
4. Richard A. Mollin, *A brief history of Factoring and primality testing B.C. (Before Computers)*, Mathematics Magazine, Vol. 75, 18-29 (2002.). doi:10.1080/0025570X.2002.11953094/
5. F. Proth, *Mémoires présentés*, C.R. Acad. Sci. Paris 87 (1878.), 374
6. R. Banov, *Veliki jezični modeli – potraga za umjetnom inteligencijom*, Poučak br. 102, 2025, str. 25 - 33.
7. A. Dujella, *Teorija brojeva*, Školska knjiga, Zagreb, 2019.
8. <https://mathworld.wolfram.com/PépinsTest.html> (5. 12. 2025)
9. <https://oeis.org/A129802> (5. 12. 2025)
10. N. Marco, A.J. Stylianides, *An exploration into the nature of ChatGPT's mathematical knowledge*, International Journal of Mathematical Education in Science and Technology, Vol. 56, (2025.) 2279-2297, doi:10.1080/0020739X.2025.2543817
11. D. Anh-Hoang, V. Tran, L. M. Nguyen, *Survey and analysis of hallucinations in large language models: attribution to prompting strategies or model behavior*, Frontiers in Artificial Intelligence, Vol. 8, (2025.) 1-21.