Tko je prvi...
dokazao osnovni teorem aritmetike?

Franka Miriam Brueckler, Zagreb

Slika 1. Šal faktorizacije prirodnih brojeva do 40 (ideja, izrada i slika: ©F. M. Brueckler)

Osnovni teorem aritmetike zasigurno je dobro poznat svakom čitatelju MiŠa:

Svaki se prirodan broj može na jedinstven način, do na poredak faktora, prikazati kao umnožak prostih faktora. Ako različite proste brojeve prikažemo različitim bojama, a složene u bojama njihovih faktora, osnovni teorem aritmetike za prirodne brojeve do 40 ilustriran je slikom 1.

Iako dosta intuitivan i, za razliku od mnogih drugih teorema, dio sadržaja osnovnoškolske matematike, ovaj je teorem relativno mlad, ako to gledamo iz perspektive kad je prvi puta u potpunosti dokazan, a opet jako star, ako gledamo iz perspektive kad su iskazani i dokazani prvi njemu srodni rezultati. Stoga, prije nego otkrijemo točan odgovor na pitanje iz naslova, pozabavit ćemo se kratkom pričom o ovom temeljnom teoremu o prirodnim brojevima.

Prvi koji su se bavili prostim brojevima bili su **pitagorejci** u 6. st. pr. Kr. Njihova i saznanja grčkih matematičara 5. i 4. st. pr. Kr. nalazimo u 7., 8. i 9. knjizi Euklidovih *Elemenata* (oko 300. pr. Kr., slika 2). U 7. knjizi Euklid daje dokaze da vrijedi:

Propozicija. *Ako neki prost broj mjeri umnožak dvaju brojeva, onda mjeri bar jednog od njih. Svaki broj je ili prost ili se može izmjeriti nekim prostim brojem.*

Slika 2. Fragment Euklidovih *Elemenata* (izvor: Wikipedia)

Pritom treba imati na umu da su za antičke grčke matematičare "brojevi" isključivo prirodni brojevi, a geometrijska interpretacija računskih operacija implicira korištenje izraza "može se izmjeriti" umjesto danas uobičajenog "je djeljiv". Iz navedene propozicije lako bi se dokazao osnovni teorem aritmetike, no Euklid ga nigdje nije iskazao niti dokazao.

U 9. pak knjizi Euklid daje dokaz sljedeće propozicije:

Propozicija. *Najmanji zajednički višekratnik skupa prostih brojeva ne može se izmjeriti nikojim drugim prostim brojem.*

Drugim riječima, Euklid je znao dokazati tvrdnju osnovnog teorema aritmetike, ali samo za prirodne brojeve čiji se svi prosti faktori pojavljuju samo po jednom.

doc. dr. sc. Franka Miriam Brueckler, Zavod za matematičku analizu, PMF – Matematički odsjek Sveučilišta u Zagrebu, fmbquak@gmail.com

Dugo vremena nakon Euklida ništa se bitno nije događalo ne samo vezano za ovaj teorem, nego – s izuzetkom Diofanta, vjerojatno u 3. st. n. e. – ni općenito u teoriji brojeva. Prvi značajniji novi doprinosi sežu u doba tzv. arapske matematike. Vezano za osnovni teorem aritmetike treba posebno istaknuti al-Fārisīja. Perzijski matematičar **Kamāl al-Dīn al-Fārisī** živio je otprilike od 1260. do 1320. godine i najpoznatiji je po svojim doprinosima optici. Manje je poznato da je u svom djelu *Tadhkirat al-Ahbāb fībayān al-tahābb*, u kojem se bavi prijateljskim brojevima[1], vezano za taj svoj interes dokazao propoziciju koju bismo moderno formulirali ovako:

Propozicija. *Svaki prirodan broj je ili prost ili se može rastaviti na konačno mnogo prostih faktora. Složen broj nema drugih djelitelja osim onih koji su umnošci tih prostih faktora.*

Vidimo da se radi o egzistencijskom dijelu osnovnog teorema aritmetike. Kod al-Fārisīja nedostaje iskaz i dokaz jedinstvenosti faktorizacije. Postoje rasprave zašto je al-Fārisī nije dokazao[2], no iz njegovog se teksta vidi da je toga bio svjestan. Vrlo sličan rezultat iskazao je i dokazao francuski svećenik i matematičar **Jean Prestet** (1648.–1691.) u svom djelu *Nouveaux Elemens de Mathématiques* (1689). Godine 1770. je pak veliki **Leonhard Euler** (1707.–1783.) iskazao kako egzistenciju faktorizacije, tako i njezinu jedinstvenost, no njegovi su dokazi nepotpuni. Nešto kasnije, 1798., **Adrien-Marie Legendre** (1752.–1833.) je dokazao egzistencijski dio, dok je jedinstvenost iz njegovih dokaza lako izvesti, no nigdje ju nije eksplicitno dokazao.

Slika 3. Portret C. F. Gauša, isječak iz slike G. Biermanna (izvor: Wikipedia)

Nekoliko godina kasnije veliki je **Carl Friedrich Gauß** (1777.–1855.) u svom znamenitom djelu *Disquisitiones Arithmeticae* (1801.) konačno dao prvi jasan iskaz i potpun dokaz osnovnog teorema aritmetike. Dakle, odgovor na pitanje iz naslova je: Gauß!

Čitatelja kojeg zanimaju pojedinosti o povijesti osnovnog teorema aritmetike upućujemo na članak A. G. Agargün, E. M. Özkan: *A Historical Survey of the Fundamental Theorem of Arithmetic* (Historia Mathematica 28 (2001.), 207–214).

[1] Dva prirodna broja su prijateljska ako je svaki od njih zbroj pravih djelitelja onog drugog.

[2] Vidi članak: A.G. Agargün, C. R. Fletcher: *al-Fārisī and the fundamental theorem of arithmetic*, Historia Mathematica (1994.) 162–173.