PSEUDOPROSTI BROJEVI

ANA JURASIĆ I MARKO RUKAVINA

Sažetak. U članku ćemo dati pregled dijela spoznaja o pseudoprostim brojevima, odnosno složenim brojevima koje se jednostavno može opisati kao nusproizvod potrage za prostim brojevima. Kroz njihovu vezu s Malim Fermatovim teoremom, odgovorit ćemo na nekoliko zanimljivih pitanja o ovoj temi.

Ključne riječi: prosti brojevi, pseudoprosti brojevi, Mali Fermatov teorem.

1. UVOD

Teorija brojeva grana je matematike koja se prvenstveno bavi svojstvima cijelih brojeva, dakle elemenata skupa

$$\mathbb{Z} = \{..., -3, -2, -1, 0, 1, 2, 3, ...\}.$$

Veliki matematičar Carl Friedrich Gauss nazivao je ovo područje aritmetikom, a poznata je njegova izreka:

"Matematika je kraljica znanosti, a aritmetika je kraljica matematike."

Netko bi mogao pomisliti da se radi o vrlo jednostavnoj grani matematike, no riječ je o iznenađujuće dubokom području koje krije brojne neriješene probleme. Mnogi od njih odnose se na proste brojeve.

Definicija 1. *Prirodan broj p nazivamo* ***prostim brojem*** *ako je $p \geq 2$ i jedini pozitivni djelitelji od p su 1 i p. Prirodan broj n nazivamo* ***složenim brojem*** *ako je $n \geq 2$ i n nije prost.*

Pitanje je li određeni veliki prirodni broj n prost ili složen jedno je od najvažnijih u teoriji brojeva, a često se javlja na primjer u kriptografiji[1]. U primjenama se najčešće zadovoljavamo brojevima za koje je vrlo velika vjerojatnost da su prosti. Testovi prostosti su kriteriji za koje vrijedi da ako ih n ne zadovolji, onda je sigurno složen, a ako ih zadovolji, onda postoji vrlo velika vjerojatnost da je prost. Što više testova "prođe", to je veća vjerojatnost da je n prost. Postoje i metode kojima je moguće egzaktno dokazati da je neki broj prost, no vjerojatnosni testovi puno su brži od svih poznatih metoda za dokazivanje prostosti. Neki teoremi u potpunosti karakteriziraju proste brojeve. Takav je na primjer ***Wilsonov teorem***:

Prirodan broj p je prost ako i samo ako p dijeli[2] $(p-1)! + 1$.

No, ovakve kriterije nije lako provjeriti za velike prirodne brojeve. Mnogi efikasniji testovi prostosti u osnovi su slični onome koji proizlazi iz Malog Fermatova teorema, što ćemo opisati u nastavku. Uvedimo najprije pojam kongruencije.

[1] Šifriranje ili kriptografija je znanstvena disciplina koja se bavi proučavanjem metoda za slanje poruka u takvom obliku da ih samo onaj kome su namijenjene može pročitati. Jedno je od glavnih područja primjene teorije brojeva.

[2] Kažemo da je cijeli broj k djeljiv s nenul cijelim brojem l, odnosno da l dijeli k, ako postoji cijeli broj x takav da je $k = lx$. To zapisujemo s $l|k$. Ako k nije djeljiv s l, pišemo $l \nmid k$.

Definicija 2. *Neka su k i l cijeli brojevi te neka je m nenul cijeli broj. Kažemo da je k* ***kongruentan*** *l* ***modulo*** *m, što označavamo s $k \equiv l \pmod{m}$, ako $m|k-l$. U protivnom, kažemo da k nije kongruentan l modulo m i pišemo $k \not\equiv l \pmod{m}$.*

Na primjer, $25 \equiv 1 \pmod{4}$ jer $4|24$, ali $25 \not\equiv 2 \pmod{4}$ jer $4 \nmid 23$. Kako $m|k-l$ ako i samo ako $-m|k-l$, bez smanjenja općenitosti uzimamo da je $m \in \mathbb{N}$. Kongruencija i jednakost dijele mnoga zajednička svojstva.

Propozicija 1. *Neka su k i l cijeli brojevi. Vrijedi:*
*1) $k \equiv k \pmod{m}$ (**refleksivnost**),*
*2) ako je $k \equiv l \pmod{m}$, tada je $l \equiv k \pmod{m}$ (**simetričnost**),*
*3) ako je $k \equiv l \pmod{m}$ i $l \equiv q \pmod{m}$, tada je $k \equiv q \pmod{m}$ (**tranzitivnost**).*

Dokaz: Pokušajte sami ili pogledajte [7, Propozicija 2.1.]. □

Propozicija 2. *Neka su k, l, q, r cijeli brojevi. Ako je $k \equiv l \pmod{m}$ i $q \equiv r \pmod{m}$, tada vrijedi:*
1) $k+q \equiv l+r \pmod{m}$ i $k-q \equiv l-r \pmod{m}$,
2) $kq \equiv lr \pmod{m}$.

Dokaz: 1) Dovoljno je dokazati slučaj sa zbrajanjem. Vrijedi $m|k-l$ i $m|q-r$ pa $m|(k-l)+(q-r)$. Dakle, $m|(k+q)-(l+r)$ pa je $k+q \equiv l+r \pmod{m}$.
2) Kako $m|k-l$ i $m|q-r$, vrijedi i $m|q(k-l)+l(q-r)$. Budući da je $q(k-l)+l(q-r) = kq-lr$, imamo $kq \equiv lr \pmod{m}$. □

Takozvana ***Kineska slutnja***:

"Prirodni broj p je prost ako i samo ako vrijedi $2^p \equiv 2 \pmod{p}$",

koja se pogrešno pripisuje drevnim Kinezima i o čijem porijeklu postoje brojne legende i nagađanja, točna je samo u jednom smjeru. Navedena kongruencija vrijedi za svaki prost broj p, kao što ćemo vidjeti u nastavku, ali ako ona vrijedi ne znači da je broj p prost. Sarrus je 1819. godine pronašao kontraprimjer $2^{341} \equiv 2 \pmod{341}$, ali je $341 = 11 \cdot 31$. Ako je p neparan broj, kongruenciju iz Kineske slutnje možemo zamijeniti s $2^{p-1} \equiv 1 \pmod{p}$. Neparne složene brojeve n za koje je

$$2^{n-1} \equiv 1 \pmod{n} \tag{1}$$

nazivamo **pseudoprostim brojevima**, a koriste se i nazivi Pouletovi brojevi, Sarrusovi brojevi itd. Kongruencija (1) vrijedi i za složene brojeve 561, 645, 1105, 1729, 1905... . Za svaki neparan prost broj vrijedi (1). Dakle, ako za neparan prirodan broj n ne vrijedi (1), n je složen. To je mogući prvi korak testa prostosti.

2. Pseudoprosti brojevi u bazi a

Postoje važna svojstva prostih brojeva koja su vrlo jednostavna za provjeru, ali ih posjeduju i neki složeni brojevi. Tipičan primjer takvog svojstva dan je u ***Malom Fermatovu teoremu***:

Neka je p prost broj. Tada za svaki cijeli broj a, takav da su a i p relativno prosti[3]*, vrijedi*

$$a^{p-1} \equiv 1 \pmod{p}. \tag{2}$$

[3]Kažemo da su cijeli brojevi k i l relativno prosti ako je njihov najveći zajednički djelitelj, kojeg označavamo s (k,l), jednak 1. Ako je $(a,p) = d > 1$, ne vrijedi (2).

Za svaki cijeli broj a vrijedi $a^p \equiv a \pmod{p}$.

Dokaz ovog teorema [7, Teorem 2.10.] mnogo je jednostavniji od dokaza Velikog (posljednjeg) Fermatova teorema[4], ali ima dalekosežnije posljedice s primjenom u kriptografiji. Da vrijedi obrat ovog teorema, imali bismo jednostavan i brz način dokazivanja prostosti. No, p može biti složen, a da ipak za neki (ili čak za svaki) a vrijedi relacija (2). To je malo vjerojatno, ali moguće. Mali Fermatov teorem ponekad se naziva i Fermatov test složenosti jer se njime može dokazati da je broj n složen. Ako je na primjer $2^{n-1} \equiv 1 \pmod{n}$, ali $3^{n-1} \not\equiv 1 \pmod{n}$, kao što vrijedi za $n = 341$, tada n nije prost. Uvedimo stoga sljedeći pojam.

Definicija 3. *Neparan složen broj n koji zadovoljava kongruenciju*

$$a^{n-1} \equiv 1 \pmod{n}, \tag{3}$$

*gdje je $a \neq 1$ cijeli broj i $(a, n) = 1$, nazivamo **pseudoprostim brojem u bazi** a (kraće* psp(a)*).*

Pseudoprost broj u bazi a "ponaša se" kao prost, time što prolazi test (3). Ovakvi se brojevi nazivaju i Fermatovim pseudoprostim brojevima. Pouletovi brojevi, na primjer 341, su pseudoprosti u bazi 2. Obično se nazivaju pseudoprostim brojevima i najviše su proučavani. Broj n za koji se ne zna da je složen i koji zadovoljava kongruenciju (3) za neku netrivijalnu bazu ($a \neq 1$) nazivamo vjerojatno prostim. Postojanje pseudoprostih brojeva u bazi a pokazuje da testiranje samo s jednom bazom nije dovoljno da bismo zaključili da je broj prost. Na primjer, $4^{14} \equiv 1 \pmod{15}$, ali 15 nije prost broj. Zato možemo kombinirati više baza. Na primjer, $3^{90} \equiv 1 \pmod{91}$ pa je 91 psp(3). No, 91 nije psp(2) jer $2^{90} \not\equiv 1 \pmod{91}$. Tako doznajemo da je broj 91 složen ($91 = 7 \cdot 13$), bez da ga faktoriziramo. Pomerance, Selfridge i Wagstaff složili su tablicu najmanjih pseudoprostih brojeva u bazama 2, 3, 5 i 7, zasebno i istodobno (Tablica 1).

Postoje i brojevi (najmanji od njih je 561) koji su pseudoprosti u svakoj bazi.

Definicija 4. *Složen broj n nazivamo **Carmichaelovim brojem** ako za svaki cijeli broj a, takav*[5] *da je $1 < a < n$ i $(a, n) = 1$, vrijedi (3).*

Carmichael je našao prvih 15 ovakvih brojeva i pretpostavio da ih ima beskonačno mnogo. Prvih nekoliko Carmichaelovih brojeva su 561, 1105, 1729, 2465, 2821, 6601, 8911, 10585, 15841, 29341, ... Može se dokazati da je svaki Carmichaelov broj neparan. Za takve brojeve ne može se koristeći Mali Fermatov teorem dokazati da su složeni. Dakle, obrat Malog Fermatova teorema ne vrijedi, kao ni obrat Kineske slutnje koja je njegov poseban slučaj. Doduše, obrat Malog Fermatova teorema, vrijedi [3, Theorem 24.1.] u sljedećem smislu:

Ako je $n \geq 2$ i za svaki cijeli broj a takav da je $1 \leq a \leq n-1$ vrijedi (3), tada je n prost.

No, da bismo provjerili da li je n prost, koristeći ovaj teorem, morali bismo se uvjeriti da (3) vrijedi za $a = 1, 2, ..., n-1$, što je za veliki n mnogo posla. Kako onda koristeći Mali Fermatov teorem ispitati je li određeni veliki neparni prirodni broj n

[4]Veliki Fermatov teorem kaže da jednadžba $x^n + y^n = z^n$ nema rješenja (x, y, z) u prirodnim brojevima kada je n prirodan broj veći od 2. Dokazao ga je Andrew Wiles 1993. godine, više od 350 godina nakon što ga je Fermat formulirao.

[5]Svaki $y \in \mathbb{Z}$ kongruentan je modulo n točno jednom broju $a \in \{0, 1, ..., n-1\}$ (ovaj skup nazivamo sustavom najmanjih nenegativnih ostataka modulo n) pa ako (3) vrijedi za neki a, onda vrijedi i za svaki $y \in \mathbb{Z}$ takav da je $y \equiv a \pmod{n}$.

TABLICA 1. Najmanji pseudoprosti brojevi u bazama 2, 3, 5 i 7

Baza a	Najmanji psp(a)	Rastav na proste faktore
2	341	$11 \cdot 13$
3	91	$7 \cdot 13$
5	217	$7 \cdot 31$
7	25	$5 \cdot 5$
$2, 3$	1105	$5 \cdot 13 \cdot 17$
$2, 5$	561	$3 \cdot 11 \cdot 17$
$2, 7$	561	$3 \cdot 11 \cdot 17$
$3, 5$	1541	$23 \cdot 67$
$3, 7$	703	$19 \cdot 37$
$5, 7$	561	$3 \cdot 11 \cdot 17$
$2, 3, 5$	1729	$7 \cdot 13 \cdot 19$
$2, 3, 7$	1105	$5 \cdot 13 \cdot 17$
$2, 5, 7$	561	$3 \cdot 11 \cdot 17$
$3, 5, 7$	29341	$13 \cdot 37 \cdot 61$
$2, 3, 5, 7$	29341	$13 \cdot 37 \cdot 61$

prost? Možemo odabrati proizvoljni cijeli broj a, takav da je $1 < a < n$. Koristeći Euklidov algoritam [7, Teorem 1.5.], odredimo $d = (a, n)$. Ako je $d > 1$, našli smo netrivijalan djelitelj d od n pa n nije prost. Ako je $d = 1$, ispitamo vrijedi li (3). Ako (3) ne vrijedi, n je složen. Ako (3) vrijedi, nastavljamo provjeru za drugi a. S daljnjom provjerom povećava se vjerojatnost da je n prost. Ako je n prošao test (3) za velik broj različitih a-ova, možemo "s velikom vjerojatnošću"[6] tvrditi da je n prost (osim ako je n pseudoprost za sve baze). Ova se metoda traženja prostih brojeva zove vjerojatnosna metoda. Razlikuje se od deterministčkih metoda, koje sa stopostotnom sigurnošću utvrđuju da li je n prost.

Zapitajmo se sada koliko ima pseudoprostih brojeva u bazi a? Erdős je dokazao da su pseudoprosti brojevi u bazi a "rjeđi" među prirodnim brojevima od prostih brojeva. Ipak, i njih ima beskonačno mnogo.

Teorem 1. *Za svaki prirodan broj $a \geq 2$ postoji beskonačno mnogo pseudoprostih brojeva u bazi a.*

Dokaz: Neka je p proizvoljan neparan prost broj koji ne dijeli $a^2 - 1$. Promotrimo[7] prirodan broj $n = \frac{a^{2p}-1}{a^2-1}$. Kako vrijedi

$$n = \frac{a^p - 1}{a - 1} \cdot \frac{a^p + 1}{a + 1},$$

slijedi da je n složen broj. Iz Malog Fermatova teorema i Propozicije 2 slijedi $a^{2p} \equiv a^2 \pmod{p}$. Dakle, p dijeli $a^{2p} - a^2 = (n - 1)(a^2 - 1)$. Kako $p \nmid a^2 - 1$, zaključujemo da $p|n - 1$. Osim toga, $n - 1 = a^{2p-2} + a^{2p-4} + ... + a^2$ je zbroj od

[6]Postoji 455052511 neparnih prostih brojeva $p \leq 10^{10}$, za koje je $2^{p-1} \equiv 1 \pmod{p}$. Postoje 14884 složena broja $2 < n \leq 10^{10}$, za koje vrijedi (1). Dakle, ako je $2 < n \leq 10^{10}$ i za n vrijedi (1), vjerojatnost da je n prost je $\frac{455052511}{455052511+14884} \approx 0.999967$, što je prilično velika vjerojatnost.

[7]Koristimo formule: $(x^n - y^n) : (x - y) = x^{n-1} + x^{n-2}y + x^{n-3}y^2 + ... + xy^{n-2} + y^{n-1}$, $n \in \mathbb{N}$, te $(x^{2n+1} + y^{2n+1}) : (x + y) = x^{2n} - x^{2n-1}y + x^{2n-2}y^2 - ... - xy^{2n-1} + y^{2n}$, $n \in \mathbb{N}$.

$p-1$ pribrojnika iste parnosti pa je $n-1$ paran broj. Dakle, $2p|n-1$ pa, kako je $a^{2p} \equiv 1 \pmod{n}$, vrijedi i (3). To znači da je n psp(a). Kako ima beskonačno mnogo prostih brojeva, ima i beskonačno mnogo pseudoprostih brojeva u bazi a.□

Neka $C(x)$ označava broj Carmichaelovih brojeva koji su $\leq x$. Tada, za svaki dovoljno veliki x vrijedi [1] $C(x) > x^{\frac{2}{7}}$, što dokazuje da postoji beskonačno mnogo Carmichaelovih brojeva. Zahvaljujući sve moćnijim računalima, znanstvenici danas otkrivaju sve veće Carmichaelove brojeve.

Postoji mnogo načina za formiranje rastućih nizova pseudoprostih brojeva u bazi a. U sljedećoj propoziciji dat ćemo jedan od njih za slučaj $a = 2$.

Propozicija 3. *Ako je n pseudoprost broj, tada je $n' = 2^n - 1$ također pseudoprost.*

Dokaz: Kako je n pseudoprost, on dijeli $2^{n-1} - 1$ pa dijeli i $2^n - 2 = n' - 1$. Dakle, $n' - 1 = k \cdot n$, gdje je $k \in \mathbb{N}$. Sada imamo:

$$2^{n'-1} - 1 = (2^n - 1)(2^{n(k-1)} + 2^{n(k-2)} + \cdots + 2^n + 1).$$

Dakle, $n' = 2^n - 1$ dijeli $2^{n'-1} - 1$ pa je i n' pseudoprost broj. □

1962. godine Crocker je pronašao sljedeći beskonačan niz pseudoprostih brojeva u bazi a. Neka je a paran broj koji nije oblika 2^{2^r}, gdje je $r \geq 0$. Tada je, za svaki $n \geq 1$, broj $a^{a^n} + 1$ pseudoprost u bazi a.

Navedimo još svojstava pseudoprostih brojeva u bazi a i Carmichaelovih brojeva.

Teorem 2. *Neka je n neparan složen broj. Tada vrijedi:*
1) n je psp(a)*, gdje je $(a, n) = 1$, ako i samo ako red*[8] *od a modulo n dijeli $n - 1$.*
2) Ako je n psp(a_1) *i* psp(a_2)*, onda je on i* psp($a_1 a_2$) *te* psp($a_1 a_2^{-1}$).
3) Ako n ne zadovoljava kongruenciju (3) za neki a, onda n ne zadovoljava (3) za barem pola mogućih baza a (tj. cijelih brojeva a takvih da je $(a, n) = 1$ i $1 < a < n$).

Dokaz: 1) Neka je d red od a modulo n i neka je n je psp(a). Pretpostavimo da je $n - 1 = d \cdot q + r$, $0 \leq r < d$ i $d, q, r \in \mathbb{Z}$. Tada je

$$a^r = a^{n-1-dq} = a^{n-1}(a^d)^{-q} \equiv 1 \pmod{n}.$$

Kako je d minimalan, r može biti jedino 0, odnosno $d|n-1$. Obrnuto, neka je $n - 1 = d \cdot q$. Tada je $a^{n-1} = (a^d)^q \equiv 1 \pmod{n}$ pa je n je psp(a).
2) Za $a = a_1$ i $a = a_2$ vrijedi (3) pa, iz Propozicije 2, slijedi $(a_1 a_2)^{n-1} \equiv 1 \pmod{n}$ i $(a_1 a_2^{-1})^{n-1} = a_1^{n-1}(a_2^{n-1})^{-1} \equiv 1 \pmod{n}$. Dakle, tvrdnja vrijedi.
3) Neka su $a_1, a_2, \ldots, a_s$ baze u kojima n jest, a neka je a' baza u kojoj n nije pseudoprost. Kongruencija (3) ne vrijedi za $a = a' a_i$, gdje je $i \in \{1, ..., s\}$, jer bi onda vrijedila i za $a' = (a' a_i) a_i^{-1}$. Dakle, postoji barem s baza u kojima n nije pseudoprost. □

1971. godine Lieuwens je pokazao da, za svaki $k \geq 2$ i za svaki $a > 1$, postoji beskonačno mnogo pseudoprostih brojeva u bazi a koji su umnošci k različitih prostih brojeva. Baillie, Wagstaff i Monier neovisno su dokazali [8] da ako je n složen broj, tada je broj baza a u kojima je n pseudoprost (kraće $B_{psp}(n)$), gdje je $1 \leq a \leq n-1$, jednak $B_{psp}(n) = \prod_{p|n}(n-1, p-1) - 1$. Slijedi da ako je n neparan

[8]Neka su $a, n \in \mathbb{N}$ i $(a, n) = 1$. Red od a modulo n je najmanji $d \in \mathbb{N}$ takav da je $a^d \equiv 1 \pmod{n}$.

složen broj, koji nije potencija od 3, tada je n pseudoprost u barem dvije baze a, takve da je $1 \leq a \leq n-1$.

Znamo li faktorizirati n, ***Korseltovim kriterijem*** možemo utvrditi je li on Carmichaelov:

> *"Prirodan broj n je Carmichaelov ako i samo ako je n složen, kvadratno slobodan*[9] *i za svaki prost faktor p od n vrijedi $p-1|n-1$."*

Slijedi da je n umnožak barem tri različita prosta broja. Zaista, kako je n kvadratno slobodan, umnožak je različitih prostih brojeva. Uzmimo da je $n = pq$, gdje su p i q prosti te je $p < q$. Tada je $n-1 = pq-1 \equiv p-1 \pmod{q-1}$. Kako je $p-1 < q-1$ imamo $p-1 \not\equiv 0 \pmod{q-1}$ pa dobivamo suprotnost s Korseltovim kriterijem. Primjer konstrukcije Carmichaelovih brojeva je Chernickova konstrukcija iz 1939. godine, koja kaže da ako je $6k+1$, $12k+1$, $18k+1$, gdje je $k \geq 1$, trojka prostih brojeva, njihov je umnožak Carmichaelov broj. Pomnožimo li dobiveni broj s $36k+1$, ako je i to prost broj, dobivamo drugi Carmichaelov broj s 4 prosta faktora. Na primjer, za $k = 1$ dobivamo Carmichaelove brojeve $1729 = 7 \cdot 13 \cdot 19$ i $63973 = 7 \cdot 13 \cdot 19 \cdot 37$. Vidimo da jedan Carmichaelov broj može dijeliti drugi. Carmichaelov broj može biti i umnožak dva Carmichaelova broja. Na primjer $N_1 = 7 \cdot 13 \cdot 19$ i $N_2 = 37 \cdot 73 \cdot 109$ su Carmichaelovi, a to je i broj $N_1 N_2$.

3. Zaključak

Postojanje Carmichaelovih brojeva pokazuje važan nedostatak testiranja prostosti na osnovu Malog Fermatova teorema. Malim modificiranjem testa taj se nedostatak može ukloniti. To vodi do razmatranja različitih vrsta pseudoprostih brojeva, što ostavljamo za proučavanje onima koje smo zainteresirali ovom temom.

Napomena: Članak je nastao iz završnog rada studenta Marka Rukavine, pod mentorstvom dr. sc. Ane Jurasić, na preddiplomskom studiju matematike Odjela za matematiku Sveučilišta u Rijeci.

Literatura

[1] W.R. ALFORD, A. GRANVILLE, C. POMERANCE, *There are Infinitely Many Carmichael Numbers*, Ann. Math. 139, 703-722, 1994.
[2] E. BACH, J. SHALLIT, *Algorithmic Number Theory, Volume 1: Efficient Algorithms*, The MIT Press, London, 1996.
[3] W. E. CLARK, *Elementary Number Theory*, Department of Mathematics University of South Florida, Tampa, 2003., http://shell.cas.usf.edu/∼wclark/elem_num_th_book.pdf
[4] L.E. DICKSON, *History of the Theory of Numbers, Vol. 1: Divisibility and Primality*, New York: Dover, 2005.
[5] A. DUJELLA, *Skripta iz kriptografije*, http://web.math.hr/∼duje/kript/kriptografija.html
[6] A. DUJELLA, *Teorija brojeva u kriptografiji*, http://web.math.hr/∼duje/tbkript/tbkriptlink.pdf
[7] A. DUJELLA, *Uvod u teoriju brojeva (skripta)*, http://web.math.hr/∼duje/utb/utblink.pdf
[8] N. KOBLITZ, *A Course in Number Theory and Cryptography*, Springer-Verlag, New York, 1994.
[9] P. RIBENBOIM, *The New Book of Prime Number Records*, Springer-Verlag, New York, 1996.

[9] Prirodan broj n je kvadratno slobodan ako je 1 najveći kvadrat koji dijeli n.

Ana Jurasić, viši asistent,
Odjel za matematiku Sveučilišta u Rijeci,
Omladinska 14, 51000 Rijeka, Hrvatska
E-mail adresa: ajurasic@math.uniri.hr

Marko Rukavina, student,
Prirodoslovno-matematički fakultet, Matematički odsjek,
Bijenička 30, 10000 Zagreb, Hrvatska