REŠETO ZA ISKANJE PRAŠTEVILSKIH DVOJČKOV

SREČKO LAMPRET

Osnovna šola Vuzenica

Math. Subj. Class. (2010): 11A41

V članku izpeljemo novo karakterizacijo praštevilskih dvojčkov. S tem rezultatom dobimo elementarno metodo za iskanje praštevilskih dvojčkov do poljubno izbranega naravnega števila.

SIEVING TWIN PRIME PAIRS

In this paper a new characterization of twin prime pairs is obtained. This result gives us an elementary method for finding twin prime pairs up to a given integer.

Praštevilski dvojček je par praštevil oblike $(p, p+2)$. Razen 2 in 3 ima vsako praštevilo obliko $6k-1$ ali $6k+1$. Zato je vsak praštevilski dvojček, razen $(3,5)$, oblike $(6k-1, 6k+1)$ za neko naravno število k. V tem članku predstavljamo elementarno metodo za iskanje praštevilskih dvojčkov do poljubnega naravnega števila, ki temelji na spodnjih rezultatih.

Lema 1. *Naj bo p praštevilo oblike $p = 6j+1$ ali $p = 6j-1$. Potem za vsako naravno število i*

$$(6(pi+j)-1,\ 6(pi+j)+1) \ \textit{in}\ (6(pi-j)-1,\ 6(pi-j)+1)$$

nista praštevilska dvojčka.

Dokaz. Najprej predpostavimo, da je $p = 6j+1$. Potem sta $6(pi+j)+1 = 6pi+p = p(6i+1)$ in $6(pi-j)-1 = 6pi-p = p(6i-1)$ sestavljeni števili za vsako naravno število i. Podobno, če je $p = 6j-1$, vidimo, da sta $6(pi+j)-1$ in $6(pi-j)+1$ sestavljeni števili za vsako naravno število i.∎

Izrek 2. *Naj bo k naravno število. Potem $(6k-1, 6k+1)$ ni praštevilski dvojček natanko tedaj, ko obstaja praštevilo $p \leqslant \sqrt{6k+1}$ oblike $6j \pm 1$ in tako naravno število i, da je $k = pi+j$ ali $k = pi-j$.*

Dokaz. Najprej predpostavimo, da $(6k-1, 6k+1)$ ni praštevilski dvojček. Potem bodisi $6k-1$ ali $6k+1$ ni praštevilo.

Oglejmo si primer, ko $6k-1$ ni praštevilo. Potem obstaja tako praštevilo $p \leq \sqrt{6k-1} \leq \sqrt{6k+1}$, da p deli $6k-1$. Zato $p \neq 2, 3$. Po izreku o deljenju z ostankom obstajata taki nenegativni celi števili n, r, da je $k = pn+r$ in

$0 \leqslant r < p$. Posledično velja $p \mid 6(pn+r)-1 = 6pn+(6r-1)$ in zato $p \mid 6r-1$. Ker je $6r-1 = pt$ za neko naravno število t in $r < p$, vidimo, da je

$$t = \frac{6r-1}{p} < \frac{6p-1}{p} < 6.$$

Zato je $t \in \{1,2,3,4,5\}$ in $6r - tp = 1$. To pomeni, da sta 6 in t tuji si števili in potemtakem $t = 1$ ali $t = 5$. Ker $p \neq 2,3$, velja bodisi $p = 6j-1$ ali $p = 6j+1$ za neko naravno število j.

Sprva si oglejmo primer, ko je $p = 6j-1$. Če je $t = 5$, sledi $1 = 6r-5p \equiv p \pmod 6$, kar je nemogoče. Torej $t = 1$ in zato je $p = 6r-1$. Potem velja $r = j$ in zato je $k = pi+j$ za $i := n$. Pri tem velja, da je $i > 0$, kajti če bi bil $i = 0$, bi veljalo $k = r$ in zato $6k-1 = 6r-1 = p$, kar nas privede do protislovja.

Sedaj si oglejmo primer, ko je $p = 6j+1$. Če je $t = 1$, sledi $p = 6r-1 \equiv -1 \pmod 6$, kar je nemogoče. Torej $t = 5$ in zato $6r-1 = 5p = 30j+5$. Tako je $r = 5j+1 = p-j$ in zato $k = pn+p-j = pi-j$ za $i := n+1 > 0$.

V primeru, ko $6k+1$ ni praštevilo, dokaz poteka podobno.

Obratna implikacija sledi iz leme 1. ∎

Sledi opis delovanja algoritma oz. rešeta za iskanje praštevilskih dvojčkov do poljubnega naravnega števila n.

1. Napravimo seznam naravnih števil $k = 1, 2, \ldots, \left\lceil \frac{n}{6} \right\rceil$.

2. Poiščemo vsa praštevila $3 < p \leqslant \sqrt{n}$.

   Pomagamo si lahko z Eratostenovim rešetom. Tako kot pri Eratostenovem rešetu tudi tu zadošča izvajati algoritem le tako dolgo, dokler praštevila ne dosežejo vrednosti $\sqrt{n}$, saj v vsaki faktorizaciji vsaj en faktor ne presega tega števila.

3. Za vsako praštevilo $3 < p \leqslant \sqrt{n}$ naredimo sledeče:

   - če $6 \mid p+1$, potem $j = \frac{p+1}{6}$, sicer $j = \frac{p-1}{6}$;
   - prečrtamo vsa števila $k = pi+j$ in $k = pi-j$ za vsak $i = 1, 2, \ldots$ z našega seznama.

4. Vsako preostalo naravno število k s seznama nam da praštevilski dvojček $(6k-1, 6k+1)$.

Sklicujoč se na izrek 2, s to metodo dobimo vse praštevilske dvojčke do n, razen para (3, 5). V naslednjem primeru predstavimo konkretno delovanje tega algoritma za $n = 250$.

Primer 1. Poiščimo vse praštevilske dvojčke do 250. Napravimo seznam naravnih števil $k = 1, 2, \ldots, 42$. Nato poiščemo vsa praštevila $3 < p \leq \sqrt{250}$. V našem primeru so to $5, 7, 11, 13$.

(i) Za $p = 5 = 6 \cdot 1 - 1$ velja $j = 1$ in zato iz našega seznama prečrtamo vsa naravna števila k oblik $5i - 1$ in $5i + 1$.

(ii) Za $p = 7 = 6 \cdot 1 + 1$ velja $j = 1$ in zato iz našega seznama prečrtamo vsa naravna števila k oblik $7i - 1$ in $7i + 1$.

(iii) Za $p = 11 = 6 \cdot 2 - 1$ velja $j = 2$ in zato iz našega seznama prečrtamo vsa naravna števila k oblik $11i - 2$ in $11i + 2$.

(iv) Za $p = 13 = 6 \cdot 2 + 1$ velja $j = 2$ in zato iz našega seznama prečrtamo vsa naravna števila k oblik $13i - 2$ in $13i + 2$.

1	2	3	~~4~~	5	~~6~~	7	~~8~~	~~9~~	10
~~11~~	12	~~13~~	~~14~~	~~15~~	~~16~~	17	18	~~19~~	~~20~~
~~21~~	~~22~~	23	~~24~~	25	~~26~~	~~27~~	~~28~~	~~29~~	30
~~31~~	32	33	~~34~~	~~35~~	~~36~~	~~37~~	38	~~39~~	40
~~41~~	~~42~~								

Za vsako preostalo naravno število k iz našega seznama dobimo praštevilski dvojček $(6k - 1, 6k + 1)$. Če dodamo še par $(3, 5)$, dobimo vse praštevilske dvojčke do 250:

$$(3,5), (5,7), (11,13), (17,19), (29,31), (41,43), (59,61), (71,73),$$
$$(101,103), (107,109), (137,139), (149,151), (179,181), (191,193),$$
$$(197,199), (227,229), (239,241).$$

Obstajajo tudi nekateri drugi algoritmi za iskanje praštevilskih dvojčkov, ki pa večinoma niso elementarni. Pri drugih, ki so elementarni, pa je, če hočemo poiskati praštevilske dvojčke do nekega poljubnega naravnega števila n, ponavadi treba najprej poiskati vsa praštevila do n in nato med njimi po raznih metodah črtamo vsa tista praštevila, ki niso del dvojčka. Pri algoritmu, ki je tu predstavljen, pa lahko poiščemo vse praštevilske dvojčke do n, pri tem pa je predhodno (npr. z Eratostenovim rešetom) treba poiskati le praštevila do $\sqrt{n}$, kar je za dovolj velike n lahko precejšnja prednost.

Zahvala. Avtor se zahvaljuje dr. Danielu Eremiti za strokovne nasvete in tehnično pomoč pri nastajanju članka. Zahvaljuje se tudi recenzentu za koristne predloge in skrbno branje članka.