PROSTI BROJEVI

1. Definicija prostog i složenog broja. Euklidov dokaz o beskonačnosti skupa prostih brojeva. Eratostenovo sito.

Za prirodni broj $p > 1$ kažemo da je **prost broj** (prim-broj) ako su mu jedini djelitelji 1 i p (tj. ima samo trivijalne djelitelje). Za broj $a > 1$ koji nije prost broj (tj. posjeduje ne trivijalne djelitelje) kažemo da je **složen broj**.

(Euklid) „*Skup svih prostih brojeva je beskonačan.*"

Dokaz:

Dokaz ćemo provesti kontradikcijom (od suprotnog). Pretpostavljamo dakle suprotno, tj. da je skup P dvih prostih brojeva konačan: $P = \{p_1, \dots, p_k\}$. Tvrdnja će biti dokazana ako uspijemo dobiti proturječje (kontradikciju). Pogledajmo broj

$$a = p_1 p_2 \dots p_k + 1.$$

On nije djeljiv niti sa kojim od p-ova, jer je ostatak pri dijeljenju sa p_i jednak uvijek 1. Prema Osnovnom teoremu aritmetike, a ima rastav na proste faktore $a = q_1^{\alpha_1} \dots q_n^{\alpha_n}$. Niti koji od prostih brojeva q_i nije u P, a to je proturječje s definicijom skupa P.

Eratostenovo sito predstavlja jednostavan postupak kojim proste brojeve dobivamo tako da u N križamo 1 i sve one brojeve koji su složeni:

1. križamo broj 1;
2. zaokružimo broj 2 i križamo sve njegove višekratnike koji ga slijede: 4,6...; broj 2 je prost;
3. prvi preostali broj je 3, zaokružimo ga i križamo sve njegove višekratnike koji ga slijede: 6,9,12..; 3 je prost broj;
4. 4 je već prekrižen, kao i svi njegovi višekratnici; itd.

Zaokruženi brojevi koji preostaju su upravo prosti brojevi. Primijetimo da ako gledamo samo konačan poskup skupa prirodnih brojeva, npr. od 1 do 10^6, onda je postupak opisan Eratostenovim zapravo algoritam (tj. završava u konačno mnogo koraka), i Eratistenovo sito može se programirati.

2. Osnovni teorem aritemetike. Citirajte ga i dokažite.

(Rastav na proste djelitelje, Osnovni teorem aritmetike)

„*Za svaki prirodni broj a > 1 postoji jedincat rastav na proste djelitelje*

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k},$$

gdje su $p_1 < p_2 < \dots < p_k$ svi različiti prosti brojevi koji dijele a, poredani po veličini. pritom α_i zovemo kratnošću odgovarajućeg prostog broja p_i u rastavu."

Dokaz:

Sastoji se od 2 dijela; prvi dio je dokaz da postoji faktorizacija, a drugi da je ona jedinstvena.

1)

Neka je q_1 najmanji prosti faktor od a, tj. $a = q_1 a_{1.}$ Sada potražimo najmanji prosti faktor od a_1, neka je to q_2: $a_1 = q_2 a_2 \Rightarrow a = q_1 q_2 a_2$. Taj postupak nastavljamo dalje, najmanji prosti faktor od a_2... Zbog činjenice da su a_1, a_2, a_3,... međusobno djelitelji unazad, $a > a_1 > a_2 > a_3 > \cdots \geq 1$. $q_1 q_2 q_3 \ldots q_n \times 1$. Ovo je rastav broja a na proste faktore ⇒ postoji rastav na proste faktore. Pritom neki prosti faktori mogu biti isti, pa se njihovim međusobnim množenjem dobije $a = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$, gdje je p_i za iste faktore.

2)

Treba pokazati da je faktorizacija jedinstvena. Pretpostavimo da faktorizacija nije jedinstvena, da za neki prirodni broj a postoje 2 različite faktorizacije:

$$a = \underbrace{q_1 q_2 \ldots q_m}_{L} = \underbrace{r_1 r_2 \ldots r_n}_{D}, \quad (m \geq n\ ili\ m \leq n)$$

$$q_1 | L \Rightarrow q_1 | D \Rightarrow q_1 = r_1,$$
$$(neki\ od\ r - ova, ne\ nužno\ r_1 \rightarrow stavimo\ ga\ na\ prvo\ mjesto)$$

Onda možemo kratiti q_1 i r_1

$$q_2 q_3 \ldots q_m = r_2 r_3 \ldots r_n, \qquad q_2 | L \Rightarrow q_2 | D \Rightarrow q_2 = r_2$$

$$q_3 \ldots q_m = r_3 \ldots r_m$$

Postupak nastavljamo dok ne dođemo do:

a) $m < n$

$$1 = r_l \ldots r_n \Rightarrow r_l = r_n = 1$$

To znači da su faktorizacije jednake → kontradikcija

b) $m > n$

$$q_l \ldots q_m = 1 \Rightarrow q_l = \cdots = q_m = 1$$

Jednake faktorizacije → kontradikcija

c) $m = n$

$$q_m = r_n$$

odma iste faktorizacije → kontradikcija

3.Dokažite da $\sqrt{2}$ i $log\,2$ nisu racionalni brojevi.

a)

Pretpostavimo da je $\sqrt{2}$ racionalan broj, što znači da postoje prirodni brojevi m i n takvi da $\sqrt{2} = \frac{m}{n}$, i da su m i n relativno prosti. Onda je $2 = \left(\frac{m}{n}\right)^2 = \frac{m^2}{n^2}$. Iz toga slijedi da je $m^2 = 2n^2$. Vidljivo je da je m^2 paran broj jer je jednak $2\mathrm{n}^2$ a on je paran jer sadrži 2. Ako je m^2 paran onda je i m paran i može se zamjeniti sa $2k$ i ubaciti u formulu

$$m^2 = 2n^2 \Leftrightarrow (2k)^2 = 2n^2 \Leftrightarrow 4k^2 = 2n^2 \Leftrightarrow 2k^2 = n^2.$$

Sada je vidljivo da je i n^2 paran, tj. da je i n paran što se neslaže sa pretpostavkom da su m i n relativno prosti. Tako smo dobili kontradikciji i dokazali suprotno: da je $\sqrt{2}$ iracionalan broj.

b)

Dokažimo da je $\log 2$ iracionalan broj. U suprotnom bi postojali prirodni brojevi m i n takvi da $\log 2 = \frac{m}{n}$. Onda je $10^{\frac{m}{n}} = 2$, tj. $10^m = 2^n$, tj. $2^m 5^m = 2^n$. To je međutim protuslovlje s Osnovnim teoremom aritmetike, jer on tvrdi da je rastav prirodnog broja na proste djelitelje jedincat.

4. Definicija funkcije τ. Izračunajte koliko djelitelja ima prirodni broj n.

Definicija:

Ukupan broj pozitivnih djelitelja prirodnog broja n se označava sa τ(n).

Teorem:

Ako je $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$, tada je:

$$\tau(n) = (\alpha_1 + 1) \times (\alpha_2 + 1) \times \dots \times (\alpha_k + 1).$$

Dokaz:

Broj n ima k različitih faktora potencije prostih brojeva, a djelitelja s bazom p_1 $\left(p_1^1 p_1^2 \dots p_1^{\alpha_1}\right)$ ima α_1. Kako je $p_1^0 = 1$ djelitelj, djelitelja ima $\alpha_1 + 1$. Ista stvar je sa bazom p_2, ...

$$(\alpha_1 + 1) \times (\alpha_2 + 1) \times \dots \times (\alpha_k + 1).$$

Prema osnovnom teoremu kombinatorike, svih mogućih djelitelja ima produkt djelitelja.

5. Definicija funkcije π i Mobiusove funkcije μ. Neke činjenice o tim funkcijama.

Definicija:

Funkcija π govori o tome koliko ima prostih brojeva.

$$\pi(x) \stackrel{\text{def}}{=} \text{broj prostih brojeva manjih ili jednakih x.}$$

Poznat je rezultat: $\pi(x) \approx \frac{x}{\ln x}$.

Definicija:

Möbiusova funkcija $\mu : N \to P$ je funkcija koja prirodnom broju n s pripadnim rastavom na proste djelitelje $n = p_1^{\alpha_1} \ldots p_k^{\alpha_k}$ pridružuje vrijednosti:

$$\mu(n) = \begin{cases} (-1)^k, & ako\ je\ \alpha_1 = \cdots = \alpha_k = 1 \\ 0, & inače. \end{cases}$$

Također definiramo $\mu(1) = 1$. Riječima, ako n posjeduje djelitelj koji je kvadrat nekog prirodnog broja većeg od 1, onda je vrijednost Möbiusove funkcije jednaka 0, a inače ± 1, ovisno o tome je li ukupan broj prostih djelitelja paran ili neparan. Npr. $\mu(4) = (2^2) = 0, \mu(6) = (2 \times 3) = (-1)^2 = 1, \mu(30) = (2 \times 3 \times 5) = (-1)^3 = -1$.

Činjenice:

O Möbiusovoj funkciji:

Za svaki prirodni broj $n > 1$ vrijedi da je

$$\sum_{d|n} \mu(d) = 0$$

gdje je d pozitivni djelitelj broja n.

(Möbiusov teorem inverzije) „*Zadane su dvije funkcije $f, g : N \to R$. Ako za svaki $n \in N$ vrijedi*

$$f(n) = \sum_{d|n} g(d),$$

onda je

$$g(n) = \sum_{d|n} \mu(d) f\left(\frac{n}{d}\right)$$

i obratno."

6. Definicija Eulerove funkcije φ. Teorem o vrijednosti $\varphi(n)$ i dokaz njegovih posljedica.

Definicija:

Funkcija $\varphi : N \to N$ koja prirodnom broju n pridružuje broj prirodnih brojeva koji su $< n$ i relativno prosti sa n zove se Eulerova funkcija. Definiramo $\varphi(1) = 1$.

Teorem:

Ako n ima rastav na proste faktore $n = p_1^{\alpha_1} \dots p_l^{\alpha_l}$, onda je

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\dots\left(1 - \frac{1}{p_l}\right).$$

Dokaz:

Na formulu $n = \sum_{d|n} \varphi(d)$ možemo primijeniti teorem inverzije, stavljajući

$f(n) = n \ i \ g(n) = \varphi(n)$. Onda je

$$\begin{aligned}\varphi(n) = \sum_{d|n} \mu(d)\frac{d}{n} &= n - \sum_{i} \frac{n}{p_i} + \sum_{i<j} \frac{n}{p_i p_j} - \cdots \\ &= n\left(1 - \frac{1}{p_1}\right)\dots\left(1 - \frac{1}{p_l}\right).\end{aligned}$$

Svojstva Eulerove funkcije:

a) $\sum_{d|n} \varphi(\mathrm{d}) = \mathrm{n}$ (**Gaussova formula**) - suma je po svim djeliteljima d broja n

b) $\mathrm{a}^{\varphi(\mathrm{n})} \equiv 1 \pmod{\mathrm{n}}$ za Nzm (a, n) = 1 (**Eulerova kongruencija**)

c) $\varphi(\mathrm{m\,n}) = \varphi(\mathrm{m})\,\varphi(\mathrm{n})$ za Nzm (m, n) = 1 (**multiplikativnost**)

d) $\varphi(\mathrm{p}) = \mathrm{p} - 1$ ako je p prost broj

e) Ako je p prost broj, onda za svaki a $\in$ N vrijedi da je: $\mathrm{a}^{\mathrm{p}} \equiv \mathrm{a} \pmod{\mathrm{p}}$.

U specijalnom slučaju kad a nije višekratnik od p je: $\mathrm{a}^{\mathrm{p}-1} \equiv 1 \pmod{\mathrm{p}}$.

(**mali Fermatov stavak**)