UVOD U TEORIJU BROJEVA

Drugo predavanje - 10.10.2013.

Prosti brojevi

Definicija 1.4. Prirodan broj $p > 1$ zove se **prost** ako nema niti jednog djelitelja d takvog da je $1 < d < p$. Ako prirodan broj $a > 1$ nije prost, onda kažemo da je **složen**.

Teorem 1.8 Svaki prirodan broj $n > 1$ može se prikazati kao umnožak prostih brojeva (s jednim ili više faktora).

Dokaz:
Koristimo matematičku indukciju. Broj 2 je prost. Pretpostavimo da je $n > 2$ i da tvrdnja teorema vrijedi za svaki prirodni broj m, takav da je $2 \leq m < n$. Dokažimo da se i n može prikazati kao umnožak prostih faktora.

Ako je n prost, nemamo što dokazivati. Ako nije, onda vrijedi $n = n_1 n_2$, gdje je $1 < n_1 < n$ i $1 < n_2 < n$. Po pretpostavci indukcije, n_1 i n_2 su umnošci prostih brojeva pa slijedi da i n ima to svojstvo. ■

Iz Teorema 1.8 slijedi da svaki prirodan broj n možemo prikazati u obliku

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r},$$

gdje su $p_1, ..., p_r$ različiti prosti brojevi, a $\alpha_1, ..., \alpha_r$ prirodni brojevi. Ovakav prikaz broja n zvat ćemo **kanonski rastav** broja n na proste faktore.

Propozicija 1.9. Ako je p prost broj i $p|ab$, onda $p|a$ ili $p|b$. Općenitije, ako $p|a_1 a_2 ... a_n$, onda p dijeli barem jedan faktor a_i.

Dokaz:
Neka $p|ab$ i $p \nmid a$. Dakle, $(p, a) = 1$, pa postoje cijeli brojevi x i y takvi da je $ax + py = 1$. Pomnožimo li tu jednakost s b, dobivamo $abx + pby = b$ pa, kako $p|ab$, slijedi da $p|b$.

Općenitiju tvrdnju dokazujemo indukcijom. Pretpostavimo da tvrdnja vrijedi za umnoške s manje od n faktora. Sada, ako $p|a_1(a_2 \cdots a_n)$, onda $p|a_1$ ili $p|a_2 \cdots a_n$. Ako $p|a_2 \cdots a_n$, onda po pretpostavci indukcije $p|a_i$ za neki $i = 2, ..., n$. ■

Teorem 1.10. (Osnovni teorem aritmetike) Faktorizacija svakog prirodnog broja $n > 1$ na proste faktore jedinstvena je do na poredak prostih faktora.

Dokaz:
Pretpostavimo suprotno, da n ima dvije različite faktorizacije. Nakon dijeljenja s prostim brojevima koji su zajednički objema faktorizacijama, dobivamo jednakost oblika

$$p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s,$$

gdje su p_i za $i = 1, ..., r$ i q_j za $j = 1, ..., s$ prosti brojevi, ne nužno različiti, ali takvi da se niti jedan prost broj s lijeve strane ne pojavljuje na desnoj strani jednakosti, tj. $p_i \neq q_j$ za sve i, j. Iz toga slijedi da $p_1 | q_1 q_2 \cdots q_s$ pa Propozicija 1.9. povlači da p_1 dijeli barem jedan q_j. Kako se radi o prostim brojevima, moralo bi vrijediti $p_1 = q_j$. Dakle, dobili smo kontradikciju.■

Analogon Teorema 1.10. ne vrijedi za cijele brojeve u (nekim) kvadratnim poljima. (O tome ćemo detaljnije kada se budemo bavili kvadratnim poljima.) Primjer nejednoznačne faktorizacije na proste faktore u prstenu $\mathbb{Z}[\sqrt{-6}] = \{a + b\sqrt{-6} : a, b \in \mathbb{Z}\}$ su dvije različite faktorizacije broja 10. Naime, vrijedi

$$10 = 2 \cdot 5 = (2 + \sqrt{-6})(2 - \sqrt{-6}).$$

Radi jednostavnosti, često ćemo prirodan broj a pisati u obliku

$$a = \prod_p p^{\alpha(p)},$$

gdje je $\alpha(p) \geq 0$. Pritom podrazumijevamo da je $\alpha(p) = 0$, za skoro sve proste brojeve p. Posebno, ako je $a = 1$ onda je $\alpha(p) = 0$ za svaki p.

Ako je $a = \prod_p p^{\alpha(p)}$, $b = \prod_p p^{\beta(p)}$, $c = \prod_p p^{\gamma(p)}$ i $ab = c$, iz Teorema 1.10. slijedi da je $\alpha(p) + \beta(p) = \gamma(p)$ za sve p. Dakle, ako $a|c$, tada je $\alpha(p) \leq \gamma(p)$ za svaki p. Obratno, ako je $\alpha(p) \leq \gamma(p)$ za svaki p, onda možemo definirati prirodan broj $b = \prod_p p^{\beta(p)}$ sa $\beta(p) = \gamma(p) - \alpha(p)$. Tada je $ab = c$ pa $a|c$. Iz prethodnog razmatranja zaključujemo da vrijedi

$$a|c \Leftrightarrow \alpha(p) \leq \gamma(p), \tag{1}$$

za svaki p. Iz (1) dalje slijedi sljedeća važna formula

$$(a, b) = \prod_p p^{\min\{\alpha(p), \beta(p)\}}. \tag{2}$$

Uvedimo sada još jedan pojam.

Definicija 1.5. Neka su $a_1, a_2, ..., a_n$ cijeli brojevi različiti od 0. Najmanji prirodan broj c za koji vrijedi da $a_i | c$ za sve $i = 1, 2, ..., n$ zove se **najmanji zajednički višekratnik** brojeva $a_1, a_2, ..., a_n$. Označavamo ga s $[a_1, ..., a_n]$.

Iz (1) slijedi da je

$$[a, b] = \prod_p p^{\max\{\alpha(p), \beta(p)\}}. \tag{3}$$

Propozicija 1.11. Vrijedi

$$(a, b) \cdot [a, b] = |ab|.$$

Dokaz:
Po definiciji su $(a, b), [a, b] \in \mathbb{N}$ pa je to razlog zbog kojeg se na desnoj strani jednakosti koju moramo dokazati stavlja apsolutna vrijednost. Po Teoremu 1.10 i formulama (2) i (3), dovoljno je provjeriti da za sve nenegativne cijele brojeve x, y vrijedi

$$\min\{x, y\} + \max\{x, y\} = x + y.$$

Ako je najprije $x \leq y$, onda vrijedi $\min\{x, y\} + \max\{x, y\} = x + y$. Ako je pak $x > y$, onda je $\min\{x, y\} + \max\{x, y\} = y + x = x + y$. ■

Za prirodan broj a reći ćemo da je **(potpun) kvadrat** ako se može zapisati u obliku n^2, za neki $n \in \mathbb{N}$. Iz Teorema 1.10 slijedi da je a potpun kvadrat ako i samo ako su svi eksponenti $\alpha(p)$ parni.

Kažemo da je a **kvadratno slobodan** ako je 1 najveći kvadrat koji dijeli a. Dakle, a je kvadratno slobodan ako i samo ako su svi eksponenti $\alpha(p)$ jednaki 0 ili 1.

Ako je p prost, onda je $p^k || a$ ekvivalentno s $k = \alpha(p)$.

Primjer: Dokažite da svaki složen broj n ima prost faktor $p \leq \sqrt{n}$.

Rješenje:
Neka je p najmanji prost faktor od n. Dakle, postoji $m \in \mathbb{N}$, takav da je $n = p \cdot m$ i vrijedi $m \geq p$. Pomnožimo li tu nejednakost s p, dobivamo $n \geq p^2$ pa, kako su $n, p \in \mathbb{N}$, slijedi $\sqrt{n} \geq p$.

Ovaj primjer možemo iskoristiti za generiranje tablice prostih brojeva tzv. *Eratostenovim sitom.* Na primjer, želimo napraviti tablicu prostih brojeva ≤ 200. Napišemo sve prirodne brojeve od 2 do 200. Prekrižimo sve prave višekratnike broja 2, pa broja 3, pa broja 5. U svakom koraku, prvi neprekriženi broj je prost te u idućem koraku križamo njegove prave višekratnike. Prvi novoprekriženi broj biti će njegov kvadrat, jer su svi manji višekratnici već prekriženi. U našem slučaju, nakon križanja višekratnika od 7, 11 i 13, tablica je gotova (jer je $17 > \sqrt{200}$).

Teorem 1.12. (Euklid) Skup svih prostih brojeva je beskonačan.

Dokaz:
Pretpostavimo suprotno, da su $p_1, p_2, ..., p_k$ svi prosti brojevi. Promotrimo broj

$$n = 1 + p_1 p_2 \cdots p_k.$$

Broj n nije djeljiv niti s p_1, niti s p_2,..., niti s p_k (da je, iz prethodne jednakosti dobili bi kontradikciju da taj p_i dijeli 1 za $i \in \{1, ..., k\}$). Dakle, svaki prosti faktor od n je različit od $p_1, ..., p_k$. Budući da je n ili prost ili ima prosti faktor, u svakom slučaju dobili smo prost broj različit od $p_1, ..., p_k$, što je kontradikcija. ■

Primjer: Dokažite da, ako je broj $2^k + 1$ prost, tada je $k = 0$ ili je $k = 2^n$ za neki cijeli broj $n \geq 0$.

Rješenje:
Neka je $2^k + 1$ prost broj. Najmanji prosti broj 2 dobivamo za $k = 0$. Sljedeći prost broj 3 dobivamo za $n = 0$, odnosno $k = 1$.

Pretpostavimo suprotno, da k ima neki neparan prosti faktor p, odnosno da je $k = p \cdot m$, gdje je m prirodan broj. Tada je broj

$$2^k + 1 = (2^m)^p + 1^p = (2^m + 1)((2^m)^{p-1} - (2^m)^{p-2} + ... + 1)$$

djeljiv s $2^m + 1$ pa nije prost. Dakle, dobili smo kontradikciju. (Ovdje smo koristili genearliziranu jednakost za zbroj potencija $a^{2n+1} + b^{2n+1} = (a + b)(a^{2n} - a^{2n-1}b + ... - ab^{2n-1} + b^{2n})$, gdje je $n \in \mathbb{N}$.)

Brojevi oblika $f_n = 2^{2^n} + 1$, gdje je n nenegativan cijeli broj, zovu se **Fermatovi brojevi**. Fermat je smatrao da su svi takvi brojevi prosti. Neki od njih i jesu, pr. $f_0 = 3$, $f_1 = 5$, $f_2 = 17$, $f_3 = 257$, $f_4 = 65537$. Međutim, s nekoliko transformacija pokazat ćemo da $f_5 = 2^{32} + 1$ nije prost. Naime, vrijedi

$$\begin{aligned}
2^{32} + 1 &= 2^4 2^{28} + 1 \\
&= (641 - 5^4)2^{28} + 1 = 641 \cdot 2^{28} - 640^4 + 1 \\
&= 641 \cdot 2^{28} - (641 - 1)^4 + 1 \\
&= ... = 641(2^{28} - 641^3 + 4 \cdot 641^2 - 6 \cdot 641 + 4)
\end{aligned}$$

pa slijedi da $641 | f_5$.

Do danas nije dokazana slutnja da je samo konačno mnogo Fermatovih brojeva prosto.

Primjer: Dokažite da, ako je broj $2^n - 1$ (gdje je n prirodan broj) prost, tada je i broj n prost.

Rješenje:
Pretpostavimo da je broj n složen, odnosno da je $n = ab$, gdje su $a > 1$, $b > 1$. Sada je broj $2^n - 1 = (2^a)^b - 1^b$ djeljiv s $2^a - 1$ pa nije prost. Dakle, dobili smo kontradikciju. (Ovdje koristimo generaliziranu jednakost za razliku potencija $a^n - b^n = (a-b)(a^{n-1} + a^{n-2}b + ... + ab^{n-2} + b^{n-1})$, gdje je $n \in \mathbb{N}$).

Brojevi oblika $M_p = 2^p - 1$, gdje je p prost broj, zovu se **Mersennovi brojevi**. Neki od njih, kao na primjer $M_7 = 127$ su prosti, a neki su složeni, kao na primjer $M_{11} = 2047 = 23 \cdot 89$. Do danas nije dokazana slutnja da Mersennovih brojeva koji su prosti ima beskonačno mnogo. Najveći danas poznat Mersennov prost broj je $M_{57885161}$.