Kovina Milošević—Rakočević

STAUDT—CLAUSEN-OVA TEOREMA

Staudt [1] i *Clausen* [2] skoro istovremeno otkrili su jednu veoma interesantnu osobinu *Bernoulli*-evih brojeva, kasnije poznatu u literaturi pod imenom *Staudt—Clausen*-ova teorema. Od njenog prvog formulisanja pa do danas dokazivana je u radovima mnogih matematičara (*Sechläfli, Lucas, Saalschütz, Schwering, Radicke, Nielsen,* itd.) na razne načine, a takođe korišćena je od mnogih autora pri efektivnom izračunavanju *Bernoulli*-evih brojeva.

Iznećemo jedan od pristupačnijih načina dokazivanja ove teoreme koji se uglavnom zasniva na poznavanju izvesnih stavova iz računa sa kongruencijama a vodi svoje poreklo iz *Staudt*-ovih radova. To je nešto modifikovan *Uspensky—Heaslet*-ov [3] dokaz.

Staudt—Clausen-ova teorema formulisana je na ovaj način:

Neka je B_n n-ti Bernoulli-ev broj definisan simboličkom relacijom

$$(1+B)^n - B_n = 0$$

u kojoj, posle razvijanja, treba B^k zameniti sa B_k. Broj B_n uvek se može napisati u obliku

$$B_n = A - \frac{1}{\lambda_1} - \frac{1}{\lambda_2} - \frac{1}{\lambda_3} - \cdots - \frac{1}{\lambda_\nu},$$

gde su: A ceo broj; $\lambda_1, \lambda_2, \ldots, \lambda_\nu$ prosti brojevi koji su za jedinicu veći od delilaca broja n.

Obeležićemo sa $S_n(a)$ zbir

$$0^n + 1^n + 2^n + \cdots + (a-1)^n.$$

Neka brojevi $0, 1, 2, \ldots, a-1$, čine kompletan sistem ostataka za moduo a. Za neki drugi sistem ostataka

$$r_1, r_2, r_3, \ldots, r_a$$

za isti moduo prema definiciji imaćemo

$$r_1 \equiv 0 \pmod{a},$$
$$r_2 \equiv 1 \pmod{a},$$
$$r_3 \equiv 2 \pmod{a},$$
$$\vdots$$
$$r_a \equiv a-1 \pmod{a}.$$

Stepenujući i sabirajući redom sve ove kongruencije, dobija se

$$S_n(a) \equiv r_1^n + r_2^n + r_3^n + \cdots + r_a^n \pmod{a}.$$

U računu sa kongruencijama dokazuje se da brojevi $as_i + r_j$ $(i = 1, 2, \ldots, b;\ j = 1, 2, \ldots, a)$ čine kompletan sistem ostataka za moduo ab, ako su a i b relativno prosti brojevi, i ako

$$s_1, s_2, \ldots, s_b; \qquad r_1, r_2, \ldots, r_a,$$

predstavljaju kompletne sisteme ostataka za moduo b, odnosno za moduo a. Tada je

$$S_n(ab) \equiv \sum_{i,j} (as_i + r_j)^n \pmod{ab}$$

ili, kako je

$$as_i + r_j \equiv r_j \pmod{a}, \quad \text{tj.} \quad as_i + r_j \equiv as_i \pmod{a},$$

imaćemo

$$S_n(ab) \equiv \sum_{i,j} r_j^n \equiv b\,S_n(a) \pmod{a},$$

ili

(2) $$S_n(ab) \equiv b\,S_n(a) + a\,S_n(b). \pmod{a}$$

Na sličan način dobili bismo relaciju

(3) $$S_n(ab) \equiv b\,S_n(a) + a\,S_n(b) \pmod{b}.$$

Relacije (2) i (3) daju zajedno relaciju

$$S_n(ab) \equiv b\,S_n(a) + a\,S_n(b) \pmod{ab},$$

ili

$$\frac{S_n(ab)}{ab} - \frac{S_n(a)}{a} - \frac{S_n(b)}{b} = k \qquad (k \text{ ceo broj}).$$

Ako su a, b, c tri relativno prosta broja, očigledno je, na osnovu ovoga što smo pokazali, da će izraz

$$\frac{S_n(abc)}{abc}-\frac{S_n(ab)}{ab}-\frac{S_n(b)}{b},$$

tj.

$$\frac{S_n(abc)}{abc}-\frac{S_n(a)}{a}-\frac{S_n(b)}{b}-\frac{S_n(c)}{c}$$

biti uvek ceo broj.

Može se dokazati da je uopšte

$$\frac{S_n(abc\ldots l)}{abc\ldots l}-\frac{S_n(a)}{a}-\frac{S_n(b)}{b}-\frac{S_n(c)}{c}\ldots-\frac{S_n(l)}{l} \tag{4}$$

uvek ceo broj ako su $a, b, c, \ldots, l$ relativno prosti brojevi.

Poznato je da svaki složeni broj m možemo napisati u ovom obliku [4]

$$m=p_1^{\alpha_1}p_2^{\alpha_2}p_3^{\alpha_3}\cdots p_s^{\alpha_s},$$

gde su brojevi

$$a=p_1^{\alpha_1},\ b=p_2^{\alpha_2},\ c=p_3^{\alpha_3},\ \ldots,\ l=p_s^{\alpha_s}$$

relativno prosti. Prema relaciji (4) izraz

$$\frac{S_n(m)}{m}-\frac{S_n(p_1^{\alpha_1})}{p_1^{\alpha_1}}-\frac{S_n(p_2^{\alpha_2})}{p_2^{\alpha_2}}-\cdots-\frac{S_n(p_s^{\alpha_s})}{p_s^{\alpha_s}} \tag{5}$$

je uvek ceo broj. Ovo se može uprostiti ako primenimo izvesne stavove iz teorije kongruencija. Naime, ako su

$$r_0, r_1, r_2, \ldots, r_{p-1};$$

$$s_0, s_1, s_2, \ldots, s_{p^{\alpha-1}-1}$$

kompletni sistemi ostataka za moduo p i $p^{\alpha-1}$, tada brojevi

$$p^{\alpha-1}r_i+s_j \qquad \left\{\begin{array}{l} i=0,1,2,\ldots,p-1 \\ j=0,1,2,\ldots,p^{\alpha-1}-1 \end{array}\right.$$

čine kompletan sistem ostataka za moduo p^α. Prema tome

$$S_n(p^\alpha)\equiv\sum_{i,j}(s_j+p^{\alpha-1}r_i)^n \pmod{p^\alpha}. \tag{6}$$

Međutim, prema binomnom obrascu je

$$(s_j+p^{\alpha-1}r_i)^n=s_j^n+\binom{n}{1}s_j^{n-1}r_i p^{\alpha-1}+\binom{n}{2}s_j^{n-2}r_i^2 p^{2\alpha-2}+\ldots,$$

i za slučaj kada je $\alpha>1$ svi članovi na desnoj strani počevši od trećeg deljivi su sa p^α. Stoga je

$$(sj+p^{\alpha-1}r_i)^n\equiv s_j^n+ns_j^{n-1}r_i p^{\alpha-1} \pmod{p^\alpha}.$$

Sumirajući ovaj izraz po i ako se j smatra konstantnim, dobijamo

$$\sum_i (s_j+p^{\alpha-1}r_i)^n\equiv ps_j^n+ns_j^{n-1}\frac{p(p-1)}{2}p^{\alpha-1} \pmod{p^\alpha}.$$

Ako je p neparan broj, tada će i drugi član na desnoj strani ove relacije biti deljiv sa p^α, pa je tada

$$\sum_i (s_j+p^{\alpha-1}r_i)^n\equiv ps_j^n \pmod{p^\alpha}.$$

Sumirajući ove kongruencije po promenljivom indeksu j, imaćemo

$$\sum_{i,j}(s_j+p^{\alpha-1}r_i)^n\equiv p\sum_j s_j^n \pmod{p^\alpha},$$

ili, s obzirom na relaciju (6)

$$S_n(p^\alpha)\equiv p\,S_n(p^{\alpha-1}) \pmod{p^\alpha},$$

tj. izraz

$$\frac{S_n(p^\alpha)}{p^\alpha}-\frac{S_n(p^{\alpha-1})}{p^{\alpha-1}} \tag{7}$$

uvek je ceo broj. Na sličan način dobija se da je

$$\frac{S_n(p^{\alpha-1})}{p^{\alpha-1}}-\frac{S_n(p^{\alpha-2})}{p^{\alpha-2}}$$

ceo broj. Sabirajući relacije koje ćemo dobiti iz (7) ako α zamenjujemo redom sa $\alpha-1$, $\alpha-2$, $\alpha-3, \ldots, 1$, dolazimo do zaključka da je

$$\frac{S_n(p^\alpha)}{p^\alpha}-\frac{S_n(p)}{p}$$

uvek ceo broj. Prema tome, relacija (5) postaje

$$\frac{S_n(m)}{m}-\frac{S_n(p_1)}{p_1}-\frac{S_n(p_2)}{p_2}-\cdots-\frac{S_n(p_s)}{p_s}=\text{ceo broj}.$$

Pokazaćemo sada da je

$$S_n(p)\equiv-1 \pmod p, \quad \text{odnosno} \quad S_n(p)\equiv 0 \pmod p,$$

prema tome da li je n deljivo ili ne sa $p-1$.

Relaciju $S_n(p)\equiv-1 \pmod p$ dokazujemo služeći se *Fermat*-ovom teoremom, po kojoj je

$$a^{p-1}\equiv 1 \pmod p,$$

ako a ne deli p. Prema tome, možemo pisati

$$1^n\equiv 1,\ 2^n\equiv 1,\ \ldots,\ (p-1))^n\equiv 1 \pmod p,$$

te sabravši ove kongruencije dobijamo relaciju

$$S_n(p)\equiv p-1 \pmod p, \text{ tj. } S_n(p)\equiv -1 \pmod p.$$

Ako pođemo sada od identiteta

$$(x+1)^a-x^a=\binom{a}{1}x^{a-1}+\binom{a}{2}x^{a-2}+\cdots+\binom{a}{a-1}x+1,$$

u kome ćemo stavljati redom $x=0, 1, 2, \ldots, p-1$, dobijamo, sabirajući tako formirane jednačine,

$$p^a-p=\binom{a}{1}S_{a-1}(p)+\binom{a}{2}S_{a-2}(p)+\cdots+\binom{a}{a-1}S_1(p),$$

tj.

$$\binom{a}{1}S_{a-1}(p)+\binom{a}{2}S_{a-2}(p)+\cdots+\binom{a}{a-1}S_1(p)\equiv 0 \pmod p.$$

Odavde za $a=2, 3, \ldots, p-1$ imamo

$$\begin{aligned}&2S_1(p)\equiv 0,\\&3S_2(p)+3S_1(p)\equiv 0,\\&4S_3(p)+6S_2(p)+4S_1(p)\equiv 0 \pmod p\\&\vdots\end{aligned}$$

Prema tome, dobija se

$$S_1(p)\equiv 0,\ S_2(p)\equiv 0,\ \ldots,\ S_{p-2}(0)\equiv 0 \pmod p.$$

Ovim smo dokazali da postoji $S_n(p) \equiv 0 \pmod{p}$, za slučaj kada n nije deljivo sa $p-1$ i kada je $n < p-1$.

Ako je $n > p-1$ i nije n deljivo sa $p-1$, imamo

$$n = (p-1)\,b + r, \qquad (0 < r < p-1).$$

Prema *Fermat*-ovoj teoremi

$$C^{p-1} \equiv 1 \pmod{p} \quad (c = 1, 2, \ldots, p-1),$$

ili

$$C^{b(p-1)} \equiv 1 \pmod{p}, \quad \text{tj.} \quad C^{r+b(p-1)} \equiv C^n \equiv C^r \pmod{p}.$$

Zato možemo pisati

$$S_n(p) \equiv S_r(p) \pmod{p},$$

tj.

$$S_n(p) \equiv 0 \pmod{p}.$$

Ovim smo dokazali da je relacija

$$S_n(p) \equiv 0 \pmod{p} \tag{8}$$

ispunjena za svako n koje ne deli p.

Videli smo ranije da je

$$\frac{S_{2n}(m)}{m} - \frac{S_{2n}(p_1)}{p_1} - \frac{S_{2n}(p_2)}{p_2} - \cdots - \frac{S_{2n}(p_s)}{p_s}$$

ceo broj ako su $p_1, p_2, \ldots, p_s$ prosti delioci broja m.

S obzirom na relaciju (8), broj $\dfrac{S_{2n}(p)}{p}$ je ceo ako $2n$ ne deli $p-1$, ili je $\dfrac{S_{2n}(p)+1}{p}$ ceo broj ako $2n$ deli $p-1$. Označivši sada sa $\lambda_1, \lambda_2, \lambda_3, \ldots$ sve različite proste brojeve koji dele m i to takve da su

$$\lambda_1 - 1, \ \lambda_2 - 1, \ \lambda_3 - 1, \ \ldots$$

delioci broja $2n$, imaćemo da je

$$\frac{S_{2n}(m)}{m} + \frac{1}{\lambda_1} + \frac{1}{\lambda_2} + \frac{1}{\lambda_3} + \cdots \tag{9}$$

uvek ceo broj.

Bernoulli-evi brojevi javljaju se u zbirovima potencija prirodnih brojeva, te se definišu i relacijom

$$S_n(p)=\frac{1}{n+1}\sum_{k=0}^{n}\binom{n+1}{k}B_k\,p^{n+1-k}. \tag{10}$$

U razvijenom obliku relacija (10) glasi

$$S_n(p)=\frac{1}{n+1}B_0p^{n+1}+B_1p^n+\frac{n}{2}B_2p^{n-1}+\frac{n(n-1)}{2\cdot 3}B_3p^{n-2}$$

$$+\frac{n(n-1)(n-2)}{2\cdot 3\cdot 4}B_4p^{n-3}+\frac{n(n-1)(n-2)(n-3)}{2\cdot 3\cdot 4\cdot 5}B_5p^{n-4}$$

$$+\cdots+\frac{n(n-1)(n-2)\cdots 2}{1\cdot 2\cdot 3\cdots n}B_np,$$

ili, s obzirom da je $B_{2k+1}=0,\ k\neq 0$

$$S_n(p)=\frac{1}{n+1}B_0p^{n+1}+B_1p^n+\frac{n}{2}B_2p^{n-1}$$

$$+\frac{n(n-1)(n-2)}{2\cdot 3\cdot 4}B_4p^{n-3}+\cdots+B_np.$$

Za $n=2k$ ova relacija postaje

$$S_{2k}(p)=\frac{1}{2k+1}B_0p^{2k+1}+B_1p^{2k}+\frac{2k}{2}B_2p^{2k-1}$$

$$+\frac{2k(2k-1)(2k-2)}{2\cdot 3\cdot 4}B_4p^{2k-3}+\cdots+B_{2k}p.$$

Izabraćemo p tako da bude deljivo sa imeniteljima brojeva

$$B_0,\ B_1,\ B_2,\ B_4,\ \ldots,\ B_{2k-2},$$

a takođe i sa brojevima

$$2,\ 3,\ 4,\ \ldots,\ 2k+1.$$

Očigledno je, da će tada razlika

$$\frac{S_{2k}(p)}{p}-B_{2k} \tag{11}$$

biti ceo broj. Pored toga p je deljivo sa svima prostim brojevima $\lambda_1, \lambda_2, \lambda_3, \ldots$, koji su takvi da su

$$\frac{2k}{\lambda_1-1}, \frac{2k}{\lambda_2-1}, \frac{2k}{\lambda_3-1}, \ldots$$

celi brojevi. Stoga je, prema (9),

$$\frac{S_{2k}(p)}{p}+\frac{1}{\lambda_1}+\frac{1}{\lambda_2}+\frac{1}{\lambda_3}+\cdots$$

ceo broj ili, prema (10),

$$B_{2k}+\frac{1}{\lambda_1}+\frac{1}{\lambda_2}+\frac{1}{\lambda_3}+\cdots$$

ceo broj. Ovim je dokazana *Staudt—Clausen*-ova relacija

$$B_n=A-\frac{1}{\lambda_1}-\frac{1}{\lambda_2}-\frac{1}{\lambda_3}-\cdots,$$

gde je A ceo broj, a $\lambda_1, \lambda_2, \lambda_3, \ldots$ prosti brojevi koji su za jedinicu veći od delilaca broja n.

Kao primer posmatrajmo broj B_{16} čija je vrednost $-\frac{3617}{510}$. Napišimo sve činioce broja 16, to su: 1, 2, 4, 8, 16. Prosti brojevi koji su za jedinicu veći od ovih su: 2, 3, 5, 17. Doista je

$$B_{16}=-6-\frac{1}{2}-\frac{1}{3}-\frac{1}{5}-\frac{1}{17}.$$

Isto tako imamo za brojeve

$$B_{22}=\frac{854513}{138}=6193-\frac{1}{2}-\frac{1}{3}-\frac{1}{23},$$

$$B_{26}=\frac{8553103}{6}=1425518-\frac{1}{2}-\frac{1}{3},$$

itd.

Ako se *Bernoulli*-ev broj B_n napiše u obliku $\frac{a_n}{2b_n}$, vidimo da je imenitelj b_n potpuno definisana numerička funkcija, tj. predstavlja proizvod neparnih prostih brojeva koji su za jedinicu veći od činioca broja n, uključujući tu i sam broj n. Međutim, nemoguće je dati njen opšti oblik s obzirom da nam je još uvek nepoznata množina prostih brojeva. Što se tiče brojitelja a_n, njegovo određivanje je još komplikovanije, kao što je slučaj i sa celim brojem A koji se javlja u *Staudt—Clausen*-ovoj relaciji.

Novije rezultate u vezi sa *Staudt—Clausen*-ovom teoremom i aritmetičkim osobinama *Bernoulli*-evih brojeva nalazimo u člancima *L. Carlitz*-a [5] i *H. S. Vandiver*-a [6].

LITERATURA

[1] K. G. C. von Staudt, *Beweis eines Lehresatzes, die Bernoulli-schen Zahlen Betreffend*, Journal für die reine und angewandte Mathematik, vol. 21, 1840, p. 372—374.

[2] Th. Clausen, *Theorem*, Astronomische Nachrichten, vol. 17, 1840, p. 351—352.

[3] J. V. Uspensky, M. A. Heaslet, *Elementary Number Theory*, New York, 1939.

[4] M. S. Popadić, *Deljivost celih brojeva*, Beograd, 1959, str. 68, (*Matematička biblioteka*, sveska 9).

[5] L. Carlitz, *The Staudt-Clausen Theorem*, Mathematics Magazine, vol. 34, 1961, № 3, p. 131—146.

[6] H. S. Vandiver, *On Development in an Arithmetic Theory of the Bernoulli and Allied Numbers*, Scripta Mathematica, vol. 25, 1961, № 4, p. 273—303.