АСИМПТОТСКА ПРОЦЕНА ЗБИРА ДЕЛИТЕЉА НЕКИХ БРОЈЕВА

РАНКО БОЈАНИЋ

1. Нека је

$$\sigma(n) = \sum_{d|n} d$$

збир делитеља броја n, при чему се 1 и n рачунају као делитељи. Функција $\sigma(n)$ је мултипликативна, тј. ако је $(a, b) = 1$ тада је

$$\sigma(ab) = \sigma(a)\,\sigma(b).$$

Из дефиниције функције $\sigma(n)$ и ове њене особине следи да је за $n = \Pi\, p^{\alpha}$

$$\sigma(n) = n \prod_{p|n} \frac{1 - p^{-\alpha-1}}{1 - p^{-1}} \tag{1}$$

где $p|n$ значи да је производ узет преко свих простих делитеља броја n.

Функција $\sigma(n)$ је као и остале функције које се јављају у теорији бројева веома неправилна. Како је $1|n$ и $n|n$ то је очевидно да је

$$\sigma(n) > n. \tag{2}$$

Осим тога је [1, стр. 264]*

$$\sigma(n) = O\,(n \lg\lg n).$$

Из ових неједначина следи да количник $\sigma(n)/n$ може узети ма коју вредност размака $(1, \infty)$. Ако посматрамо известан низ целих бројева $\{a_n\}$, може се десити да $\sigma(a_n)/a_n$ тежи одређеној граници кад $n \to \infty$.

---

* Бројеви у угластим заградама односе се на литературу на крају чланка.

Проблеми ове врсте су очевидно једноставни ако знамо структуру броја a_n, као што је то случај код низова $\{p_n\}$, $\{p_1 p_2 \cdots p_n\}$, итд, где p_n означава n-ти прост број. Тако, на пример, у првом случају је $\sigma(p_n) = p_n + 1$ па према томе

$$\frac{\sigma(p_n)}{p_n} \to 1, \quad n \to \infty. \tag{3}$$

Много сложенији проблеми су они код којих делитељи посматраног низа бројева нису експлицитно дати. Такви су, на пример, низови

$$F_n = 2^{2^n} + 1, \quad M_p = 2^p - 1, \ p \text{ прост број},$$

затим $\{p_1 p_2 \cdots p_n + 1\}$, итд.

Низови $\{a_n\}$ који имају особину да $\sigma(a_n)/a_n \to 1$ нарочито су интересантни због тога што су у том случају њихови чланови у извесном смислу врло блиски простим бројевима. Пример Fermat-ових бројева $F_n = 2^{2^n} + 1$ то најбоље показује. Fermat је наиме претпостављао да су сви бројеви тог облика прости, али када је Euler нашао да је F_5 сложен број, увидело се да је Fermat-ова претпоставка погрешна и она је замењена претпоставком да простих бројева у низу $\{F_n\}$ има бесконачно много. Каснија испитивања показала су да је можда још вероватније да простих бројева у томе низу има коначно много, тим пре што до данас није нађен ниједан Fermat-ов прост број већи од F_4 [1, стр. 15]. Међутим из једног става P. Erdös-a [2] чији доказ није објављен следи да $\sigma(F_n)/F_n \to 1$, $n \to \infty$. Ако тај резултат упоредимо са (3), видећемо да се Fermat-ови бројеви у томе погледу не разликују од простих бројева.

Слично стоје ствари и са Mersenne-овим бројевима, тј. бројевима облика $M_p = 2^p - 1$, где је p прост број. До 1952 године било је познато 12 простих бројева овог облика и то оних за $p = 2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107, 127$. Те године су помоћу једне електронске машине за рачунање испитани Mersenne-ови бројеви за све експоненте $p < 2309$. Том приликом нађена су свега три нова проста броја у низу $\{M_p\}$ и то за $p = 521, 607$ и 1279. Међутим и овде $\sigma(M_p)/M_p \to 1$, $p \to \infty$, као што ћемо то показати у тачки **3.**

2. Сви низови $\{a_n\}$ који имају особину да $\sigma(a_n)/a_n \to 1$, $n \to \infty$ припадају уствари једном скупу природних бројева дефинисаном на следећи начин:

Број n припада скупу N ако његови прости делитељи задовољавају услов

(4) $$a \lg n < p, \quad a > 0.$$

То непосредно произлази из следеће једноставне леме:

Лема 1. *Ако је* $n \in N$, *тада*

$$\frac{\sigma(n)}{n} \to 1, \quad n \to \infty.$$

Доказ. Из (1) и (2) следи да је

$$1 > \frac{n}{\sigma(n)} = \prod_{p|n} \frac{1-p^{-1}}{1-p^{-\alpha-1}} \geqslant \prod_{p|n} (1-p^{-1}).$$

За $n \in N$ је према (4) $p > a \lg n$, па је

$$1 > \frac{n}{\sigma(n)} \geqslant \left(1 - \frac{1}{a \lg n}\right)^{\omega} \geqslant 1 - \frac{\omega}{a \lg n},$$

где је ω број простих делитеља броја $n \in N$. Како је

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_{\omega}^{\alpha_{\omega}} \geqslant (a \lg n)^{\omega},$$

где је p_k k-ти прост делитељ броја n, то је

$$\omega \leqslant \frac{\lg n}{\lg \lg n + \lg a},$$

па је коначно

$$1 > \frac{n}{\sigma(n)} \geqslant 1 - \frac{1}{a(\lg \lg n + \lg a)} \to 1, \quad n \to \infty.$$

Према томе, да би смо доказали да се збир делитеља броја a_n асимптотски понаша као a_n, тј. да $\sigma(a_n)/a_n \to 1$, $n \to \infty$, довољно је да докажемо да делитељи тога броја задовољавају услов (4), тј. да је $a \lg a_n < p$. Другим речима, проблем се своди на процену делитеља бројева $\{a_n\}$. У следећој тачки даћемо неколико једноставних процена те врсте.

3. (i) Нека је

$$a_n = p_1 p_2 \cdots p_n + 1,$$

где је p_n n-ти прост број. Овај низ бројева познат је још из Еуклидовог доказа да постоји бесконачно много простих бројева: наиме, из чињенице да a_n није дељиво ниједним од првих n простих бројева следи да a_n мора бити дељиво неким простим бројем који је већи од p_n или, другим речима, да сви прости делитељи броја a_n задовољавају неједначину $p > p_n$. Одатле непосредно следи да је задовољен услов (4), јер ако ставимо

$$\vartheta(x) = \sum_{p \leqslant x} \lg p,$$

тада из

$$\lg a_n = \lg(p_1 p_2 \cdots p_n + 1) \leqslant 2 \lg(p_1 p_2 \cdots p_n) = 2\vartheta(p_n)$$

и Чебишељеве неједначине $\vartheta(x) \leqslant 2x$ следи

$$\frac{1}{4} \lg a_n \leqslant p_n < p.$$

Коначно, применом претходне леме добијамо да $\sigma(a_n)/a_n \to 1$, $n \to \infty$.

(ii) Процена простих делитеља бројева M_p и F_n непосредно следи из самог облика тих делитеља.

Ако је q прост делитељ броја $M_p = 2^p - 1$, тада је q облика

$$q = 2kp + 1 \tag{5}$$

[1, стр. 79], па је према томе $q > p$. Из ове неједначине следи

$$\lg M_p = \lg(2^p - 1) \leqslant p \lg 2 \leqslant q,$$

па према претходној леми $\sigma(M_p)/M_p \to 1$, $p \to \infty$.

Целине ради, даћемо овде доказ обрасца (5). Нека је d најмањи цео број такав да је

$$2^d \equiv 1 \pmod{q}.$$

Тада је на основу Fermat-овог става $d \mid q-1$. Из претпоставке $q \mid M_p$, тј. из

$$2^p \equiv 1 \pmod{q}$$

следи да p мора бити мултипл тог најмањег експонента d, тј. да је $p = ld$, где је l цео број. Међутим, p је прост број, па је према томе $p = d$, тј. $p \mid q-1$, а тиме је образац (5) доказан.

Слично се процењују прости делитељи броја $F_n = 2^{2^n} + 1$. Наиме, ако је q прост делитељ броја F_n, тада је q облика

(6) $$q = 2^{n+1} \cdot k + 1$$

[3], па је увек $q > 2^{n+1}$, а одатле следи

$$\lg F_n = \lg (2^{2^n} + 1) \leqslant 2^n \lg 2 + 1 < 2^{n+1} < q.$$

Неједначина (4) је према томе задовољена па на основу леме 1 добијамо да

$$\sigma (F_n)/F_n \to 1, \quad n \to \infty.$$

Сам образац (6) доказује се као и у претходном случају на основу Fermat-овог става. Ако је q прост делитељ броја F_n, тада је

$$2^{2^n} \equiv -1 \pmod q),$$

тј.

(7) $$2^{2^{n+1}} \equiv 1 \pmod q).$$

Доказаћемо да је 2^{n+1} најмање решење конгруенције

$$2^m \equiv 1 \pmod q).$$

Означимо најмање решење те конгруенције са d. Тада из (7) следи да је $2^{n+1} = ld$, где је l цео број. Према томе, d може бити један од бројева $2, 2^2, \cdots, 2^{n+1}$. Међутим, конгруенција

$$2^{2^k} \equiv 1 \pmod q)$$

не може бити тачна ако је $k = 1, 2, \cdots, n$ јер десна страна обрасца

$$2^{2^k} - 1 = F_0 F_1 \cdots F_{k-1}$$

није дељива са q због тога што су сви Fermat-ови бројеви међусобно релативно прости, а q је по претпоставци делитељ од F_n. Према томе је $d = 2^{n+1}$, па је $2^{n+1} \mid q - 1$ тј. q је облика $2^{n+1} k + 1$, где је k цео број.

4. Уколико низ бројева који посматрамо има делитеља који остају ограничени, поступак из претходне тачке знатно се компликује. Овде ћемо изнети два таква случаја.

(i) Ако је p прост број $\geqslant 3$ и $N_p = 2^p + 1$, тада

(8) $$\sigma (N_p)/N_p \to \frac{4}{3}, \quad p \to \infty.$$

Један прост делитељ броја N_p је очевидно 3. Показаћемо најпре да N_p за $p > 3$ није дељиво ниједним већим степеном броја 3.

Најмањи експонент m за који је конгруенција

$$2^m \equiv 1 \pmod{3^2}$$

тачна је 6. Претпоставимо да је за неко $p > 3$ број N_p дељив са 3^2, тј. да је

$$2^p \equiv -1 \pmod{3^2}.$$

Одатле следи

$$2^{2p} \equiv 1 \pmod{3^2}.$$

$2p$ мора бити дакле мултипл од 6, тј. $2p = 6l$, односно $p = 3l$. То је међутим немогуће јер је p прост број већи од 3. Према томе, претпоставка да је за неко $p > 3$ број N_p дељив са 3^2 није тачна.

То значи да је за $p > 3$

$$N_p = 3 \cdot N_p', \quad (3, N_p') = 1.$$

Према томе је

$$\sigma(N_p) = \sigma(3)\,\sigma(N_p') = \tag{9}$$
$$= 4 \cdot \sigma(N_p').$$

Остало је још да проценимо просте делитеље броја N_p', или што је исто, просте делитеље броја N_p који су већи од 3. Претходно приметимо да је увек

$$(2^n - 1,\ 2^n + 1) = 1. \tag{10}$$

Ово је очевидно јер ако је $m \mid 2^n - 1$ и $m \mid 2^n + 1$, тада је $m \mid (2^n + 1) - (2^n - 1)$, тј. $m \mid 2$, а одатле следи да је $m = 1$ због тога што су посматрани бројеви непарни.

Прости делитељи броја $N_p = 2^p + 1$ који су већи од 3 истог су облика као и делитељи броја M_p, тј.

$$r = 2\,lp + 1, \tag{11}$$

али је доказ тога нешто сложенији.

Наиме, нека је $r \mid N_p$, $r > 3$. Тада из

$$2^p \equiv -1 \pmod{r}$$

следи

$$2^{2p} \equiv 1 \pmod{r}. \tag{12}$$

Означимо са d најмањи број такав да је

$$2^d \equiv 1 \pmod{r}.$$

Из (12) следи да је $2p = ld$, тј. да је $d = 2$, p или $2p$. Како је $r > 3$, то је $d > 2$. Осим тога, конгруенција

$$2^p \equiv 1 \pmod{r}$$

не може бити тачна јер је према (10) $(2^p - 1, 2^p + 1) = 1$. Према томе је $d = 2p$, а одатле следи (11).

Из (11) непосредно следи да прости делитељи броја N_p који су већи од 3, тј. прости делитељи броја N_p', задовољавају услов (4) па према томе

$$\sigma(N_p')/N_p' \to 1, \quad p \to \infty,$$

што заједно са (9) даје (8).

(ii) Нека су најзад p и q прости бројеви $(q \geqslant 3)$ и

$$N_{pq} = 2^{pq} + 1.$$

Овде ћемо доказати да

$$\sigma(N_{pq})/N_{pq} \to \sigma(N_p)/N_p, \quad q \to \infty. \tag{13}$$

Најтежи део доказа овог обрасца састоји се у томе да се издвоје делитељи броја N_{pq} који остају ограничени кад $n \to \infty$.

Један од делитеља броја N_{pq} је $N_p = 2^p + 1$, па је

$$N_{pq} = N_p \cdot R_{pq},$$

где је

$$R_{pq} = 2^{p(q-1)} - 2^{p(q-2)} + \cdots + 2^{2p} - 2^p + 1.$$

Доказаћемо најпре да су бројеви N_p и R_{pq} релативно прости ако је q довољно велико, а затим ћемо проценити просте делитеље броја R_{pq}. Прво тврђење непосредно следи из ове леме

ЛЕМА 2. *Ако су p и q прости бројеви, $(q \geqslant 3)$ тада је*

$$(N_p, R_{pq}) = \begin{cases} 1, & q \nmid 2^p + 1, \\ q, & q \mid 2^p + 1. \end{cases}$$

Доказ. Нека је

$$(N_p, R_{pq}) = m.$$

Тада је

$$(14)\qquad \begin{gathered} 2^p+1\equiv 0 \pmod{m}; \\ 2^{p(q-1)}-2^{p(q-2)}+\cdots+2^{2p}-2^p+1\equiv 0 \pmod{m}. \end{gathered}$$

Ову последњу конгруенцију можемо написати на следећи начин

$$(15)\qquad \begin{gathered} \{2^{p(q-1)}-1\}-\{2^{p(q-2)}+1\}+\cdots \\ \cdots+\{2^{2p}-1\}-\{2^p+1\}+q\equiv 0 \pmod{m}. \end{gathered}$$

Како међутим из прве од конгруенција (14) следи да је за $\nu=1, 2, 3, \ldots$

$$2^{2\nu p}-1\equiv 0 \text{ и } 2^{(2\nu-1)p}+1\equiv 0 \pmod{m},$$

то се (15) своди на

$$q\equiv 0 \pmod{m}.$$

Одавде, с обзиром на то да је q прост број следи да m може бити само q или 1. Да ли је

$$m=q \text{ или } m=1$$

зависи очевидно од тога да ли је конгруенција

$$(16)\qquad 2^p+1\equiv 0 \pmod{q}$$

тачна или није, а тиме је лема доказана.

Из ове леме следи да је за $q>2^p+1=N_p$

$$(17)\qquad (N_p,\ R_{pq})=1,$$

јер тада конгруенција (16) очевидно не може бити тачна, па је

$$\sigma(N_{pq})=\sigma(N_p)\ \sigma(R_{pq}).$$

Остало је још да докажемо да прости делитељи броја R_{pq} задовољавају услов (4). Како је

$$\lg R_{pq}\leqslant \lg N_{pq}=\lg(2^{pq}+1)\leqslant pq\lg 2+1\leqslant 2pq$$

тј.

$$(18)\qquad \frac{1}{2p}\lg R_{pq}\leqslant q,$$

то је очевидно довољно да докажемо да су сви прости делитељи броја R_{pq} већи од q.

ЛЕМА 3. *Ако је r прост делитељ броја R_{pq} и $q > N_p$, тада је $r > q$.*

Доказ. Нека је $q > N_p$ и $r \mid R_{pq}$. Тада је и $r \mid N_{pq}$, али је због (17) $(r, N_p) = 1$. Из $r \mid N_{pq}$, тј. из

$$2^{pq} \equiv -1 \pmod{r}$$

следи

(19) $$2^{2pq} \equiv 1 \pmod{r}.$$

Нека је d најмањи експонент такав да је

(20) $$2^d \equiv 1 \pmod{r}.$$

Тада из (19) следи да је $2pq = ld$, тј. да је

$$d = 2,\ p,\ q,\ 2p,\ 2q,\ pq \text{ или } 2pq.$$

Одмах се може видети да d не може бити ниједан од бројева

$$2,\ p,\ q,\ 2p,\ pq.$$

Наиме, за $p = 2$ из $3 \mid 2^{2q} - 1$ и (10) следи да 3 није делитељ броја $2^{2q} + 1$. За $p \geqslant 3$ из $(r, N_p) = 1$ следи да је $r > 3$. Према томе d не може бити 2. Осим тога, d не може бити ниједан од бројева p, q, pq јер би из

$$2^p \equiv 1, \quad 2^q \equiv 1, \quad 2^{pq} \equiv 1 \pmod{r}$$

следило

$$2^{pq} \equiv 1 \pmod{r},$$

а ова конгруенција није тачна због тога што је $r \mid N_{pq}$ и $(2^{pq} - 1,\ 2^{pq} + 1) = 1$. Најзад, d не може бити $2p$ јер кад би конгруенција

$$2^{2p} \equiv 1 \pmod{r}$$

била тачна, онда би из $(r, N_p) = 1$ и ове конгруенције следило

$$2^p \equiv 1 \pmod{r},$$

а то је као што смо мало пре видели немогуће.

Према томе је

$$d = 2q \text{ или } d = 2pq,$$

па је према (20)

$$2q \mid r - 1 \text{ или } 2pq \mid r - 1,$$

тј.

$$r = 2lq + 1 \text{ или } r = 2lpq + 1.$$

Дакле, у сваком случају је $r > q$, што је требало доказати.

Коначно, из ове леме и (18) следи да прости делитељи броја R_{pq} задовољавају услов (4), тј. да је

$$\frac{1}{2p}\lg R_{pq} < r.$$

Применом леме 1 добијамо да

$$\sigma(R_{pq})/R_{pq} \to 1, \; q \to \infty,$$

а тиме је образац (13) очевидно доказан.

ЛИТЕРАТУРА

[1] Hardy and Wright, The Theory of Numbers, Oxford, 1945.
[2] P. Erdös, Problem 4590, American Mathematical Monthly, vol. 61, № 5 (1954), стр. 350.
[3] L. Euler, Comm. Arith. I, стр. 55.

Ranko Bojanić

L'ÉVALUATION ASYMPTOTIQUE DE LA SOMME DE DIVISEURS DES CERTAINS NOMBRES

(Résumé)

Si l'on considère une suite infinie des nombres entiers $\{a_n\}$ on voit qu'il est possible dans certains cas d'évaluer le comportement asymptotique de $\sigma(a_n)/a_n$. Cette évaluation est évidemment simple lorsqu'on connaît explicitement les diviseurs premiers du nombre a_n, par exemple, si $a_n = p_n$ ou $a_n = p_1 p_2 \cdots p_n$, où $\{p_n\}$ est la suite des nombres premiers. Par contre, ces évaluations deviennent plus difficiles lorsqu'on ne connaît pas explicitement ces diviseurs. Dans ce dernier cas P. Erdös [2] a démontré pours les nombres de Fermat $F_n = 2^{2^n}+1$ que

$$\sigma(F_n)/F_n \to 1, \ n \to \infty.$$

On démontre ici tout d'abord que tous les nombres $\{a_n\}$ telle que

$$\sigma(a_n)/a_n \to 1, \ n \to \infty \tag{I}$$

apartiennent à un ensemble N des entiers, défini de la manière suivante: *$n \in N$ lorsque les diviseurs premiers de n satisfont à l'inégalité*

$$a \lg n < p, \quad a > 0. \tag{II}$$

Pour $n \in N$ on a alors

$$\frac{\sigma(n)}{n} \to 1, \ n \to \infty. \tag{III}$$

D'après (II) et (III) il est évident que (I) a lieu toutes les fois que $a \lg a_n < p$, $a > 0$, p étant un diviseur premier de a_n.

De cette remarque simple découle immédiatement le résultat de *M.* Erdös et en même temps les résultats analogues pour les nombres

$$a_n = p_1 p_2 \cdots p_n + 1 \ \text{ et } \ a_n = 2^{p_n} - 1.$$

On démontre de même que

$$\frac{\sigma(2^{pq}+1)}{2^{pq}+1} \to \frac{\sigma(2^p+1)}{2^p+1}, \ q \to \infty,$$

où p et q sont les nombres premiers.