Számelméleti megjegyzések II.
Az Euler-féle ϕ-függvény néhány tulajdonságáról

ERDŐS PÁL

$\phi(n)$ jelentse az Euler-féle ϕ függvényt, azaz az n-nél kisebb n-hez relatív prímszámok számát. Amint ismeretes, a $\phi(n)$ növekedése rendkívül szabálytalan. Végtelen sok n-re $\phi(n) = n-1$ (akkor és csakis akkor, ha n prímszám). *Landau*[1] viszont bebizonyította, hogy

$$\liminf_{n\to\infty} \frac{\phi(n) \operatorname{loglog} n}{n} = e^{-c}, \tag{1}$$

ahol c az Euler konstans.

Schoenberg[2] bebizonyította, hogy minden $0 < c < 1$ értékre azon számok sűrűsége, melyekre $\phi(n)/n > c$ létezik és c-nek szigorúan monoton folytonos függvénye. Az $1 \leqq a_1 < a_2 < \ldots$ egész számok sorozatának akkor mondjuk, hogy sűrűsége létezik, ha

$$\lim_{n\to\infty} A(n)/n, \quad A(n) = \sum_{a_i \leqq n} 1 \tag{2}$$

létezik. Ha a (2) alatti limesz 0, akkor a sorozat sűrűsége 0.

Legyen mármost $\phi(n) = \phi_1(n)$, $\phi_k(n) = \phi(\phi_{k-1}(n))$. $L(n)$ jelentse azt a legkisebb k számot, melyre $\phi_k(n) = 1$. *Sivasankaranarayana Pillai*[3], aki tudtommal először vizsgálta a ϕ függvény iterációját, bebizonyította, hogy

$$\left[\frac{\log n}{\log 2}\right] \geqq L(n) - 1 \geqq \left[\frac{\log \frac{n}{2}}{\log 3}\right] \tag{3}$$

[1] E. LANDAU, Verteilung der Primzahlen, Vol. 1. 216–219.

[2] I. SCHOENBERG, Über die asmptotische Verteilung reeller Zahlen mod 1. Math. Zeitschrift 28 (1928) 171–199. További idevonatkozó tételeket és problémákat lásd P. ERDŐS, On additive arithmetical functions and applications of probability to number theory, Proc. Int. Congress of Math., Amsterdam, Vol. 3 (1954) 13–19.

[3] S. SIVASANKARANARAYANA PILLAI, On a function connected with $\phi(n)$ Bull. Amer. Math. Soc. 35 (1929) 871–841.

Shapiro[4] bebizonyította, hogy az $L(n)$ függvény lényegileg multiplikatív. Érdekes lenne a következő sejtés bebizonyítása:

Létezik oly c konstans, hogy majdnem minden n-re

$$L(n) = \big(c+o(1)\big)\log n. \tag{4}$$

Azaz, más szavakkal: Minden $\varepsilon > 0$-ra azon számok sűrűsége, melyekre

$$(c-\varepsilon)\log n < L(n) < (c+\varepsilon)\log n$$

1-el egyenlő. Ha (4) igaz, úgy (3) szerint mindenesetre $\frac{1}{\log 3} \leqq c \leqq \frac{1}{\log 2}$.
(4) bebizonyítása (vagy megcáfolása) azonban igen nehéznek látszik.

Landau módszerével könnyű bebizonyítani, hogy minden fix k-ra

$$\liminf_{n\to\infty} \frac{\phi_k(n)(\log\log n)^k}{n} = e^{-kc}.$$

Ezzel szemben valószínűleg igaz a következő állítás: Minden c_1-hez létezik oly $c_2 = c_2(c_1)$, hogy az a legkisebb k szám, melyre

$$\phi_k(n) < n^{c_1}$$

nagyobb, mint $c_2 \log n$. Ennek az állításnak a bebizonyítása azonban nem látszik könnyűnek.

Schinzel[5] bebizonyította, hogy

$$\limsup_{n\to\infty} \phi_2(n)/n = \frac{1}{2},$$

és valószínűleg igaz, hogy minden k-ra

$$\limsup_{n\to\infty} \phi_k(n)/n = \frac{1}{2^{k-1}}. \tag{5}$$

(5) bebizonyítása azonban már $k = 3$-ra se sikerült nekem (triviális csak az, hogy (5) $\geqq$ jellel igaz).

E dolgozat főcélja a következő tétel bebizonyítása lesz.

TÉTEL. Majdnem minden n-re, ha $k \geqq 2$,

$$\lim_{n\to\infty} \frac{\phi_k(n)\log\log\log n}{\phi_{k-1}(n)} = e^{-c}.$$

[4] H. SHAPIRO, An arithmetic function arising from the ϕ function, Amer. Math. Monthly 50 (1943) 18–30. Lásd még *Murányi Aladár*, Az Euler-féle ϕ-függvény iterálásával nyert számelméleti függvényről, Mat. Lapok 11 (1960) 47–67 és *H. Lindren* Australian Math. Teacher, 10 (1954), 52–53, továbbá E. S. Barnes, ibid. 11 (1955), 20–21.

[5] Levélbeli közlés.

Más szóval tételünk azt jelenti, hogy minden $\varepsilon > 0$-ra azon számok sűrűsége, melyekre

$$(1-\varepsilon)e^c\phi_k(n)\log\log\log n < \phi_{k-1}(n) < (1+\varepsilon)e^c\phi_k(n)\log\log\log n$$

teljesül, 1-gyel egyenlő.

Egyszerűség kedvéért tételünket részletesen csak $k = 2$-re fogjuk bebizonyítani, $k > 2$-re csak vázolni fogjuk a bizonyítást.

Régebben bebizonyítottam[6], hogy azon $n < x$ számok száma. melyekre $\big(n, \phi(n)\big) = 1$,

$$(1+o(1))e^{-c}x/\log\log\log x. \tag{7}$$

Tételünk bizonyítása hasonlít (7) bizonyításához.

Lemma 1. Legyen $p < (\log\log n)^{1-\varepsilon}$ ($\varepsilon > 0$ fix szám). *Fennáll*

$$\Sigma' \frac{1}{q} > c_1 \frac{\log\log n}{p} > (\log\log n)^{\varepsilon/2},$$

ahol Σ'-ben q végigfut azokon a prímszámokon, melyekre $q \equiv 1 \pmod p$, $q < \exp(\log n/(\log\log n)^2)$.

$c_1, c_2, \ldots$ pozitív abszolút konstansok, $\exp z = e^z$, p és q mindig prímszámokat fognak jelenteni. 6) alatt idézett cikkemben e lemmát bebizonyítottam, itt csak a teljesség kedvéért közöljük a bizonyítást. Jelölje $\pi(x, k, l)$, $(l, k) = 1$ azon $q \leqq x$ prímszámok számát, melyekre $q \equiv l \pmod k$. *Page*[7] egy tétele szerint, ha $k < \log x$, akkor l-ben és k-ban egyenletesen fennáll, hogy

$$\pi(x, k, l) = (1+o(1))\frac{x}{\phi(k)\log x}.$$

Ezért, ha $x > \log n > e^p$

$$\pi(x, p, 1) > \frac{1}{3}\frac{x}{p\log x}. \tag{8}$$

(8)-ból egyszerű számolással nyerjük, hogy

$$\Sigma' \frac{1}{q} > \frac{1}{4p}\Sigma\frac{1}{t\log t} > c_1\frac{\log\log n}{p},$$

[6] P. Erdős, Some asymptotic formulas in number theory, Journal Indian Math. Soc. 12 (1948) 75–78.

[7] A. Page, On primes in an arithmetic progression, Proc. London Math. Soc. second series 39 (1935) 136. old. (36) formula.

ahol t a $(\log n, \exp[\log n/(\log\log n)^3])$ intervallum egész számain fut végig, ezzel lemmánk be van bizonyítva.

Jelentse $A_p(n)$ azon $m \leqq n$ számok számát, melyekre $\phi(m) \not\equiv 0 \pmod p$. Ezen m számok éppen azok, melyekre

$$p^2 \nmid m \text{ és } m \not\equiv 0 \pmod q \qquad \text{ahol } q \equiv 1 \pmod p.$$

Brun módszeréből[8] s lemmánkból, valamint *Mertens*[9] tételéből azonnal nyerjük, hogy ha $p < (\log\log n)^{1-\varepsilon}$, akkor

$$A_p(n) < c_2 n \Pi'\left(1 - \frac{1}{q}\right) < c_3 n \exp(-\log\log n)^{\varepsilon/2} = o\left(\frac{n}{\log\log n}\right), \tag{9}$$

ahol Π'-ben $q \equiv 1 \pmod p$ és $q < \exp(\log n/(\log\log n)^2)$. Itt különben sincs szükségünk a Brun-féle módszer teljes erejére, könnyű belátni, s az az egyszerűbb okoskodás, mellyel *Brun* bebizonyította, hogy az ikerprímszámok reciprok értékeinek összege konvergál, is célhoz vezet[10].

(9)-ből azonnal nyerjük, hogy

$$\sum_{p < (\log\log n)^{1-\varepsilon}} A_p(n) < (\log\log n)^{1-\varepsilon} o\left(\frac{n}{\log\log n}\right) = o(n). \tag{10}$$

(10)-ből azonnal nyerjük, hogy minden $\varepsilon > 0$-ra azon $m < n$ számok száma, melyekhez van oly $p < (\log\log n)^{1-\varepsilon}$, hogy

$$\phi(m) \not\equiv 0 \pmod p$$

$o(n)$. Azaz $o(n)$, m szám kivételével minden $m \leqq n$-re

$$\phi(m) \equiv 0 \pmod{\prod_{p < (\log\log n)^{1-\varepsilon}} p}. \tag{11}$$

(11)-ből *Mertens* tételéből nyerjük, hogy majdnem minden $m \leqq n$-re

$$\begin{aligned} \phi(\phi(m)) = \phi_2(m) \leqq \phi(m) \prod_{p < (\log\log n)^{1-\varepsilon}} \left(1 - \frac{1}{p}\right) < \\ < (1 + o(1))(1-\varepsilon) e^{-c} \phi(m)/\log\log\log m. \end{aligned} \tag{12}$$

[8] Lásd pl. P. ERDŐS, On the easier Waring problem for powers of primes, I. Proc. Cambridge Phil. Soc. 33 (1937), Lemma 2., 8. old.

[9] Lásd pl. HARDY—WRIGHT, The theory of numbers, III. kiad. 351. old.

[10] LANDAU, Vorlesungen über Zahlentheorie, Vol. 1. 75. old. vagy P. ERDŐS, Note on the number of prime divisors of integers, Journal London Math. Soc. 12 (1937) 310. old. Lemma 3.

Minthogy (12) minden ε-re igaz, nyerjük, hogy majdnem minden m-re (azaz egy 0 sűrűségű sorozat elhanyagolásával)

$$\limsup_{n\to\infty} \frac{\phi_2(m) - \log\log\log m}{\phi_1(m)} \leqq e^{-c}. \tag{13}$$

Másrészt azonban ismét *Mertens* tételéből nyerjük, hogy

$$\begin{aligned} \phi(\phi(m)) &= \phi(m) \prod_{p/\phi(m)} \left(1 - \frac{1}{p}\right) = \phi(m)\Pi_1(m)\Pi_2(m) \geqq \\ &\geqq \big(1+o(1)\big)\cdot(1+\varepsilon)^{-1}e^{-c} \frac{\phi(m)}{\log\log\log n}\, \Pi_2(m), \end{aligned} \tag{14}$$

ahol Π_1-ben p végigfut az összes prímszámokon, melyekre $p \leqq \leqq (\log\log n)^{1+\varepsilon}$ és Π_2-ben $p/\phi(m)$, $p > (\log\log n)^{1+\varepsilon}$.

Most bebizonyítjuk, hogy minden $n > 0$-ra azon $m \leqq n$ számok száma, melyekre

$$\Pi_2(m) < 1 - \eta \tag{15}$$

$o(n)$. Hogy ezt beláthassuk, elsősorban bebizonyítjuk a következő lemmát.

LEMMA 2.

$$\Sigma' \frac{1}{q} < c_4 \frac{\log p + \log\log n}{p},$$

ahol Σ'-ben $q \leqq n$, $q \equiv 1 \pmod p$.

6) alatt idézett cikkben e lemma is be van bizonyítva, teljesség kedvéért azonban közöljük a (nagyon rövid) bizonyítást.

Nyilvánvaló, hogy

$$\Sigma' \frac{1}{q} < \sum_{a=1}^{p} \frac{1}{1+ap} + \Sigma'' \frac{1}{q} < c_4 \frac{\log p}{p} + \Sigma'' \frac{1}{q},$$

ahol Σ''-ben $q \equiv 1 \pmod p$, $p^2 < q < n$. *Titchmarsh*[11] egy ismert tétele miatt, ha $x > p^2$

$$\pi(x, p, l) < c_5 \frac{x}{p \log x}. \tag{16}$$

[11] E. C. TITCHMARSH, A divisor problem, Rend. del Circ. Mat. Palermo 64 (1930) 416. old.

(16)-ból egyszerű számolás alapján nyerjük, hogy

$$\Sigma'' \frac{1}{q} < \frac{c_6}{p} \sum_{x<n} \frac{1}{x \log x} < c_4 \frac{\log\log n}{p},$$

s ezzel lemmánk be van bizonyítva.

Lemmánkból azonnal nyerjük, hogy azon $m \leqq n$ számok száma, melyekre $\phi(m) \equiv 0 \pmod p$

$$n - A_p(n) \leqq \Sigma'' \left[\frac{n}{q}\right] \leqq \Sigma' \frac{n}{q} < c_4 n \frac{\log p + \log\log n}{p}. \tag{17}$$

(17)-ből nyerjük, hogy (Π'''-ban és Σ'''-ban $(\log\log n)^{1+\varepsilon} < p \leqq n$)

$$1 \geqq \prod_{m=4}^{n} \Pi_2(m) = \Pi''' \left(1 - \frac{1}{p}\right)^{n - A_p(n)} = \exp \Sigma''' (n - A_p(n)) \log\left(1 - \frac{1}{p}\right) >$$

$$> \exp c_4 n \Sigma''' \frac{\log p + \log\log n}{p} \log\left(1 - \frac{1}{p}\right) > \tag{18}$$

$$> \exp\left\{-c_5 n \Sigma''' \frac{\log p + \log\log n}{p^2}\right\} > \exp\left(-\frac{c_6 n}{(\log\log n)^{\varepsilon}}\right).$$

(18)-ból $\Pi_2(m) \leqq 1$ miatt azonnal adódik, hogy azon $m \leqq n$ számok száma, melyekre $\Pi_2(m) < 1 - \eta$ kisebb, mint

$$\frac{c_6 n}{(\log\log n)^{\varepsilon} \log(1-\eta)} = o(n),$$

s ezzel (15) igazolva van.

(14)-ből és (15)-ből nyerjük, hogy minden $\varepsilon > 0$ és $\eta > 0$ mellett $o(n)$ számú $m \leqq n$ kivételével

$$\begin{aligned} \phi(\phi(m)) &\geqq (1 + o(1))(1+\varepsilon)^{-1}(1+\eta)^{-1} \frac{\phi(m) e^{-c}}{\log\log\log n} \geqq \\ &\geqq (1 + o(1))(1+\varepsilon)^{-1}(1+\eta)^{-1} e^{-c} \frac{\phi(m)}{\log\log\log m}, \end{aligned} \tag{19}$$

minthogy $m > \sqrt{n}$-re $\log\log\log m = \log\log\log n + o(1)$, (19)-ből nyerjük, hogy egy 0 sűrűségű sorozat elhanyagolásával

$$\liminf \frac{\phi_2(m) \log\log\log m}{\phi_1(m)} \geqq e^{-c}. \tag{20}$$

(13) és (20)-ból tételünk azonnal következik.

$k > 2$-re bizonyításunk hasonlít a $k = 2$-re való bizonyításhoz. Először bebizonyítjuk, hogy majdnem minden n-re minden $\varepsilon > 0$ mellett

$$(21) \qquad \phi_k(n) \equiv 0 \left(\mathrm{mod} \prod_{p < (\log\log n)^{k-\varepsilon}} p\right).$$

(21) bizonyításához azonban *Page* tétele nem eléggé éles, itt a *Rodosskij—Tatuzawa*[12]-féle tételek kellenek a rövid számtani sorokban levő prímszámokról.

Továbbá bebizonyítjuk, hogy majdnem minden n-re, minden $\eta > 0$ és $\varepsilon > 0$ mellett

$$(22) \qquad \prod_{\substack{p/\phi_k(n) \\ p > (\log\log n)^{k+\varepsilon}}} \left(1 - \frac{1}{p}\right) > 1 - \eta.$$

A bizonyítás nagyon hasonlít (15) bizonyításához.

(21) és (22)-ből tételünk *Mertens* tételéből azonnal következik. Tételünkből könnyen bebizonyítható, hogy

$$(23) \qquad \sum_{n=1}^{x} \phi_k(n) = (1 + o(1)) \frac{3}{\pi^2} e^{-c(k-1)} x^2 / (\log\log\log x)^{k-1}.$$

(23) bizonyítását azonban nem részletezzük.

Még néhány eredményt szeretnék bizonyítás nélkül kimondani. Jelentse $f_k(c, n)$ azon $m < n$ számok számát, melyekre $\phi_k(n)/n > c$. *Brun* módszerének segítségével nem nehéz bebizonyítani, hogy $k \geqq 3$-ra, ha n elegendő nagy,

$$f_k(c, n) < \frac{n}{(\log n)^{1+\delta}},$$

ahol $\delta > 0$ abszolút konstans. Ezzel szemben minden $c < \frac{1}{2}$-re és minden r-re

$$f_2(c, n) > n(\log\log n)^r / \log n,$$

ha $n > n_0(r)$. Továbbá minden $\varepsilon > 0$-ra, ha $n > n_0(\varepsilon)$

$$f_2(c, n) < \frac{n}{(\log n)^{1-\varepsilon}}.$$

$f_2(c, n)$-re nem sikerült aszimptotikus formulát találnom, s ez nem is látszik könnyűnek. $k \geqq 3$-ra nem tudok $f_k(c, n)$-re jó alsó becslést adni.

[12] Lásd pl. PRACHAR, Primzahlverteilung, Springer, 1957, 314—320.

Legyen $p > 2$. A q prímszámról akkor mondjuk, hogy p-re vonatkozólag az r-edik osztályban van, ha

$$\phi_r(q) \equiv 0 \pmod{p} \text{ de } \phi_k(q) \not\equiv 0 \pmod{p} \text{ ha } k < r.$$

Ha $\phi_k(q) \not\equiv 0 \pmod{p}$ minden k-ra, akkor q az ω-adik osztályban van. $f(p, r, x)$ (ill. $f(p, \omega, x)$) jelentse az x-nél kisebb és r-edik osztályban levő prímszámok számát. A számtani sorra vonatkozó prímszámtételből következik, hogy

$$f(p, 1, x) = \big(1 + o(1)\big)\frac{x}{(p-1)\log x}.$$

A számtani sorra vonatkozó prímszámtételből az eratosthenesi szita segítségével levezethető, hogy

$$f(p, 2, x) = \big(1 + o(1)\big)\frac{(p-2)x}{(p-1)\log x}.$$

Brun módszerével és a rövid számtani sorok prímszámaira vonatkozó *Rodosskij—Tatuzawa*-féle tételekből levezethető, hogy

$$\pi(x) - f(p, 1, x) - f(p, 2, x) =$$
$$= \sum_{r=3}^{\infty} f(p, r, x) + f(p, \omega, x) = o\left(\frac{x}{(\log x)^{1+\delta_p}}\right).$$

Minden valószínűség szerint minden r-re és p-re

$$\lim_{x\to\infty} f(p, r, x) = \infty, \quad \lim_{x\to\infty} f(p, \omega, x) = \infty,$$

de ezt már $r = 3$-ra se tudom bebizonyítani.

Még két, a $\phi(n)$ függvényre vonatkozó kérdést szeretnék említeni.

1. Igaz-e, hogy azon n számok sűrűsége, melyekhez nincs oly m, melyre $\phi(n) = \phi(m)$, $(n, m) = 1$ 0?

2. Igaz-e, hogy az $n - \phi(n)$ $1 \leqq n < x$ alakú különböző számok sűrűsége 0?

Az e cikkben bebizonyított és említett tételek és problémák majdnem valamennyien átvihetők a $\sigma(n)$ függvényre is, ahol $\sigma(n)$ n osztóinak összegét jelenti.

ЗАМЕЧАНИЯ ПО ТЕОРИИ ЧИСЕЛ II.

П. Ердёш

Пусть $\phi(n)=\phi_1(n)$ функция ϕ Эйлера и положим $\phi_k(n)=\phi[\phi_{k-1}(n)]$ Автор доказывает, что если пренебречь некоторой последовательностю плотности 0, тогда для $k\geqq 2$ имеет силу равенство

$$\lim_{n\to\infty}\frac{\phi_k(n)\log\log\log n}{\phi_{k-1}(n)}=e^{-c}$$

где c-постоянная Эйлера.

Ставлятся разные другие задачи и высказываются некоторые результаты, откосящиеся к функции ϕ.

REMARKS ON NUMBER THEORY II.

P. Erdős

Let $\phi(n)=\phi_1(n)$ be Euler's ϕ function and put $\phi_k(n)=\phi(\phi_{k-1}(n))$. The author proves that if we neglect a sequence of density 0 then for $k\geqq 2$

$$\lim_{n\to\infty}\frac{\phi_k(n)\operatorname{logloglog} n}{\phi_{k-1}(n)}=e^{-c},$$

where C is Euler's constant.

Several other problems and results are stated about the ϕ function.