Számelméleti megjegyzések I

ERDŐS PÁL

Legyen p prímszám és $n_2(p)$ jelentse p legkisebb quadratikus nem maradékját. Nyilvánvaló, hogy $n_2(p)$ mindig prímszám. A matematikusok több mint 150 éve foglalkoznak $n_2(p)$ megbecslésével, de a végleges megoldástól még nagyon is messze vagyunk. Az első ide vonatkozó eredmény GAUSSTÓL [1] való. A quadratikus reciprocitási tétel első bizonyításánál használt egyik segédtétele szerint, ha $p \equiv 1 \pmod 8$, akkor $n_2(p) < 2p^{\frac{1}{2}} + 1$.

A Brauer [2] elemi úton ezt az eredményt élesítette. 1917-ben VINOGRADOFF [3] bebizonyította, hogy elegendő nagy p-re

$$n_2(p) < p^{\frac{1}{4}e^{\frac{1}{2}}} (\log p)^2. \tag{1}$$

Davenport és a szerző [4] (1)-et kissé élesítették, [$\log p$ kitevőjét csökkentették). Az első lényeges javítás azonban 1957-ben BURGESS-nek [5] sikerült, aki bebizonyította, hogy minden $\varepsilon > 0$-hoz van oly $p_0 = p_0(\varepsilon)$, hogyha $p > p_0(\varepsilon)$, akkor

$$n_2(p) < p^{\frac{1}{4}e^{\frac{1}{2}}+\varepsilon} \tag{2}$$

s eddig (2) a legjobb eredmény. Valószínűnek látszik, hogy $n_2(p) = o(p^{\varepsilon})$, sőt talán elegendő nagy c-re $n_2(p) < c \log p$.

Az mindenesetre biztos, hogy ennél több nem lehet igaz, CHOWLA és TURÁN [6] egy megjegyzése szerint ugyanis van oly c, hogy végtelen sok p-re $n_2(p) > c \log p$.

LINNIK [7] „nagy szitája" segítségével bebizonyította, hogy minden ε-hoz van oly $c = c(\varepsilon)$, hogy n és n^2 között legfeljebb c oly prímszám van, melyre $n_2(p) > p^{\varepsilon}$.

E kis cikkben egy sokkal egyszerűbb problémával fogunk foglalkozni. L. MIRSKY [8] egy kérdésére válaszolva be fogjuk bizonyítani, hogy

$$\sum_{p<x} n_2(p) = (1+o(1)) \frac{x}{\log x} \sum_{k=1}^{\infty} \frac{p_k}{2^k}, \tag{3}$$

ahol $2 = p_1 < p_2 < \cdots$ a prímszámok sorozata. (3) bizonyításához LINNIK [7] módszerét fogjuk használni.

Jelölje $n_k(p), p$ legkisebb k-adik nem maradékát. Valószínűnek látszik, hogy fennáll

$$\sum_{p<x} n_k(p) = (1+o(1))c_k \frac{x}{\log x}. \tag{4}$$

(4) bizonyításának az a nehézsége, hogy $k > 2$ esetén szerző nem tud jó felső becslést azon $p < x$ prímszámok számára, melyekre $n_k(p) > A(x)$, ahol $A(x)$ x-el együtt végtelenhez tart. (4) bebizonyításához elég lenne kimutatni, hogy ezen prímszámok száma kisebb mint $c_1 \frac{x}{\log x\ A(x)^{2+c_2}}$, ennek kimutatása azonban eddig nem sikerült.

Jelentse $r(p), p$ legkisebb primitív gyökét. Nagyon nehéznek látszik

$$\sum_{p<x} r(p) = (1+o(1))c \frac{x}{\log x}$$

bebizonyítása. Még azt se sikerült bebizonyítani, hogy $r(p)$ nem tart végtelenhez p-vel együtt. ARTIN sejtette, hogy végtelen sok prímszám van, melyre 2 primitív gyök, de ennek bebizonyítása nagyon nehéznek látszik. Tudtommal még az sincs bebizonyítva, hogy minden p prímszámhoz van oly $q < p$ prímszám, mely p-nek primitív gyöke.

$r(p)$ felső becslésével többen foglalkoztak. VINOGRADOFF [9] bebizonyította, hogy $p > p_0(\varepsilon)$-ra

$$r(p) < p^{\frac{1}{2}+\varepsilon}. \tag{5}$$

HUA, H. SHAPIRO és a szerző [10](5)-öt $r(p) < c_3 p^{\frac{1}{2}} v(p-1)^{c_4}$-re javították, ahol $v(p-1)$, $p-1$ különböző prímfaktorainak számát jelenti. (5) első lényeges élesítése azonban itt is BURGESSTŐL és WANGTÓL* [11] való, akik bebizonyították, hogy $p > p_0(\varepsilon)$-ra

$$r(p) < p^{\frac{1}{4}+\varepsilon}.$$

Könnyen lehetséges, hogy $r(p) < c \log p$. (A RIEMANN sejtés helyességének feltételezése mellett ANKENY [12] bebizonyította. hogy

$$n_2(p) < c(\log p)^2).$$

A p-hez relatív prím maradékosztályok csoportja, ha $p \equiv 1 \pmod{k}$, szétesik k mellékosztályra a k-adik hatványmaradékok csoportjára vonat-

* BURGESS cikkét nem találtam, [11] alatt WANG dolgozatát citálom.

kozólag. Jelölje $A_k(p)$ azt a legkisebb pozitív egész számot, hogy valamennyi mellékosztály tartalmazza legalább egy $A_k(p)$-nál kisebb pozitív egészet. DAVENPORT és a szerző [4] bebizonyította, hogy ha $p > p_0$, akkor

$$A_k(p) < p^{\frac{1}{2}-c_k'}, \tag{6}$$

ahol $c_k' > 0$ csak k-tól függ. Valószínűnek látszik, hogy

$$\sum_{p<x} A_k(p) = (1+o(1))C_k \frac{x}{\log x}.$$

Talán itt is igaz, hogy $A_k(p) < c^{(k)} \log p$.

Most bebizonyítjuk (3)-at. Jelölje $f(k, x)$ azon p prímszámok számát x-ig, melyekre $n_2(p) = p_k$. Bebizonyítjuk, hogy fix k-ra

$$f(k, x) = (1 + o(1))\frac{x}{2^k \log x} \tag{7}$$

és hogy $p_k < \frac{1}{4} \log x$ esetén

$$\sum_{l \equiv k} f(l, x) = F(k, x) < \frac{cx}{2^{k-1} \log x}. \tag{8}$$

Legyen $n_2(p) = p_k$. Ekkor $i < k$ esetén

$$\left(\frac{p_i}{p}\right) = +1 \quad \text{és} \quad \left(\frac{p_k}{p}\right) = -1.$$

Tehát a quadratikus reciprocitási tétel szerint ha $p \equiv 1 \pmod 4$ $p_i > 2$, akkor

$$\left(\frac{p}{p_i}\right) = +1 \quad \text{és} \quad \left(\frac{p}{p_k}\right) = -1.$$

Ha $p \equiv 3 \pmod 4$, akkor $p_i > 2$ esetén

$$\left(\frac{p}{p_i}\right) = (-1)^{\frac{p_i-1}{2}} \quad \text{és} \quad \left(\frac{p}{p_k}\right) = (-1)^{\frac{p_k+1}{2}}.$$

Továbbá, ha $k > 1$ (azaz $p_k > 2$) akkor $\left(\frac{2}{p}\right) = -1$ miatt $p \equiv 3 \pmod 8$, vagy $p \equiv 5 \pmod 8$, ha $p_k = 2$, akkor $\left(\frac{2}{p}\right) = +1$ miatt $p \equiv 1 \pmod 8$, vagy $p \equiv 7 \pmod 8$.

Tehát $p \left(\mod 8 \prod_{i=2}^{k} p_i\right)$ $2 \prod_{i=2}^{k} \frac{p_i - 1}{2}$ számú számtani sorban helyezkedhet el. A számtani sorra vonatkozó prímszámtétel szerint, ha

$(\mu, p_1 \dots p_k) = 1$ a $p < x$ $p \equiv u \left(\mathrm{mod}\ 8 \prod_{i=2}^{k} p_i\right)$ prímszámok száma

$$(1+o(1)) \frac{x}{4 \prod_{i=2}^{k} (p_i - 1) \log x},$$

ebből viszont

$$f(k, x) = (1+o(1))\, 2 \prod_{i=2}^{k} \frac{p_i - 1}{2} \frac{x}{4 \prod_{i=2}^{k} (p_i - 1) \log x} - (1+o(1)) \frac{x}{2^k \log x}$$

s ezzel (7) be van bizonyítva. (7)-ből nyilván adódik, hogyha $A(x)$ x-el együtt elegendő lassan tart végtelenhez, akkor $p_k < A(x)$ esetén

$$f(k, x) = (1 + o(1)) \frac{x}{2^k \log x}.$$

Most rátérünk (8) bizonyítására. BRUN módszeréből könnyen következik [13], hogy $d < x^{\frac{1}{2}}$ esetén a $p \equiv u \pmod{d}$, $p < x$ prímszámok száma kisebb, mint

$$\frac{cx}{\phi(d) \log x}. \tag{10}$$

Jól ismert továbbá, hogy $\prod_{p<y} p < 4^y$ miatt

$$4 \prod_{p_i < \frac{1}{4} \log x} p_i < x^{\frac{1}{2}}. \tag{11}$$

(10) és (11) miatt nyerjük ugyanúgy, mint (7) bizonyításánál, hogy $p_k < \frac{1}{4} \log x$ esetén (ti. itt $n_2(p) > p_k$, azaz $i < k$-ra $\left(\frac{p_i}{p}\right) = -1$.

$$F(k, x) < 2 \prod_{i=2}^{k-1} \frac{p_i - 1}{2} \frac{cx}{4 \prod_{i=2}^{k-1} (p_i - 1) \log x} = \frac{cx}{2^{k-1} \log x}$$

s ezzel (8) is be van bizonyítva.

Fennáll nyilván

$$\sum_{p<x} n_2(p) = \sum_{p_k<x} p_k f(k, x) = \sum\nolimits_1 + \sum\nolimits_2 + \sum\nolimits_3 \tag{12}$$

ahol Σ_1-ben $2 \leqq p_k \leqq A(x)$, Σ_2-ben $A(x) < p_k < \frac{1}{4}\log x$, és Σ_3-ban $\frac{1}{4}\log x < p_k$. (9) és (12) miatt

$$(13) \qquad \sum_1 = \sum_{p_k < A(x)} (1+o(1))\frac{p_k}{2^k}\frac{x}{\log x} = \frac{x}{\log x}\sum_{k=1}^{\infty}\frac{p_k}{2^k} + o\left(\frac{x}{\log x}\right),$$

(8) és (12) és $f(k, x) \leqq Fk, x)$ miatt viszont

$$(14) \qquad \sum_2 < \frac{cx}{\log x}\sum_{A(x)<p_k}\frac{p_k}{2^{k-1}} = o\left(\frac{x}{\log x}\right).$$

(12), (13) és (14) miatt (3) bebizonyításához elég lesz

$$(15) \qquad \sum_3 = o\left(\frac{x}{\log x}\right)$$

bebizonyítása. (15) igazolásához lesz a nagy szitára szükségünk.

LEMMA 1. Legyenek $u_1 < u_2 < \cdots < u_z < N$ egész számok. Legyen $f(p)$ és $Q(p)$ két tetszőleges függvény, melyre $0 < f(p) < p$, $1 < Q(p)$ (p prímszám). Továbbá

$$\min_{p<\frac{1}{2}N^{1/3}}\frac{f(p)}{p} = \tau, \qquad \max_{p<\frac{1}{2}N^{1/3}} Q(p) = Q.$$

$Z(p, h)$ jelentse marmost az u_j ($j = 1, 2, \ldots, Z$) sorozat azon tagjainak számát, melyekre $u_j \equiv h \pmod p$. Akkor minden $p < \frac{1}{2}N^{1/3}$ prímszámra, kivéve esetleg $9NQ^2/Z\tau$ „abnormális" prímszámot, és minden $h \pmod p$ maradékosztályra kivéve esetleg $f(p)$ „abnormális" maradékosztályt, fennáll

$$\left| Z(p, h) - \frac{Z}{p} \right| < \frac{Z}{p(p)}.$$

LEMMA 1. a nagy szita RÉNYI [14] által élesített formája. Lemma 1. azt jelenti, hogyha néhány abnormális prímszámtól és maradékosztálytól eltekintünk, akkor minden maradékosztályba majdnem egyforma sok u_j esik.

LINNIK gondolatát követve Lemma 1-ből nyerjük:

LEMMA 2. $\psi(y, T)$ jelentse azon számok számát T-ig, melyeknek prímfaktorai y-nál nem nagyobbak. Fennáll

$$\sum_{k>y} f(k, x) < \frac{72x^4}{\psi(y, x^4)}$$

Legyenek ugyanis $p_1 < p_2 < \cdots < p_r \leqq x$ azon prímszámok, melyekre $n(p_i) > y$ [nyilván $r = F(y+1, x)$]. $u_1 < u_2 < \cdots < u_z$ legyenek az x^4-nél kisebb számok, melyeknek minden prímfaktora $\leqq y$, $z = \psi(y, x^4)$. Ezért tehát feltevésünk szerint $\left(\frac{u_j}{p_i}\right) = +1$ minden $1 \leqq j \leqq Z$ és $1 \leqq i \leqq r$-ra.

Ekkor azonban $Z(p_i, h) = 0$ ha h quadratikus nem maradék (mod p_i). Legyen mármost Lemma 1-ben $\tau = \frac{1}{2}$, $Q = 2$. Akkor a $p_1, p_2, \ldots, p_r$ prímszámok mindegyike abnormális s ezért Lemma 1-ből ($N = x^4$)

$$r < \frac{36\,x^4}{\psi(y, x^4)^{\frac{1}{2}}} = \frac{72\,x^4}{\psi(y, x^4)},$$

ezzel Lemma 2. be van bizonyítva.

LEMMA 3. Legyen $\varepsilon > 0$ tetszőlegesen kicsi. Tegyük fel, hogy

(17) $$\log y / \log\log w \to \infty \qquad (\text{ha } w \to \infty).$$

Akkor

$$\psi(y, w) > w^{1-\varepsilon}.$$

(17) nyilván azt jelenti, hogy $\frac{y}{(\log w)^t} \to \infty$ minden fix t-re.

Minthogy $\psi(y, w)$ y-nak nem csökkenő függvénye feltehetjük, hogy $y < w^{\varepsilon/2}$. Legyen $y^k \leqq w < y^{k+1}$. Nyilván

(18) $$y^k \geqq w^{1-\varepsilon/2}.$$

Jelölje $\pi(y)$ az y-nál nem nagyobb prímszámok számát. Ismert, hogy $\pi(y) > \frac{y}{2\log y}$. Nyilvánvaló, hogy

$$\psi(y, w) \geqq \binom{\pi(y)}{k} > \left(\frac{\pi(y)^k}{k}\right) > \frac{y^k}{(2k\log y)^k} > \frac{w^{1-\varepsilon/2}}{(2k\log y)^k} > w^{1-\varepsilon}$$

minthogy (17) és $y^k \leqq w$ miatt

$$(2k\log y)^k \leqq (2\log w)^{\log w/\log y} < w^{\varepsilon/2};$$

ezzel Lemma 3 be van bizonyítva.

LEMMA 4. Jelölje $M(x)$ azon $p < x$ prímszámok számát, melyekre $n_2(p) > (\log x)^{\log\log x}$. Fennáll

$$M(x) = o(x^\eta)$$

minden $\eta > 0$-ra.

Legyen $y = (\log x)^{\log\log x}$. Lemma 2 miatt nyilván

$$M(x) = \sum_{k<y} f(k, x) < \frac{72x^4}{\psi(y, x^4)} = o(x^\eta)$$

minthogy Lemma 3 miatt $\psi(y, x^4) > x^{4(1-\varepsilon)}$ minden $\varepsilon > 0$-ra ha x elegendő nagy. Ezzel Lemma 4. be van bizonyítva. Nyilván Lemma 4 igaz marad, ha $(\log x)^{\log\log x}$, $(\log x)^{f(x)}$-el lett volna helyettesítve, ahol $f(x) \to \infty$ x-el együtt.

Most (15)-öt könnyen be tudjuk bizonyítani. Nyilván

$$\sum_3 = \sum_3' + \sum_3'', \tag{19}$$

ahol $\sum_3'$-ben

$$\tfrac{1}{4}\log x < n_2(p) < (\log x)^{\log\log x}$$

és $\sum_3''$-ben

$$n_2(p) > (\log x)^{\log\log x}.$$

Legyen $\pi\left(\frac{\log x}{4}\right) = r > \frac{\log}{10\log\log x}$. (8)-ból nyilván következik, hogy

$$\sum_3' < (\log x)^{\log\log x} F(r, x) < \frac{cx(\log x)^{\log\log x}}{2^{r-1}\log x} = o\left(\frac{x}{\log x}\right). \tag{20}$$

(1)-ből és Lemma 4-ből viszont nyerjük, hogy

$$\sum_3'' < M(x) \max_{p<x} n_2(p) < x^{\eta+\frac{1}{2}} = o\left(\frac{x}{\log x}\right). \tag{21}$$

(19), (20) és (21)-ből (15) azonnal következik s ezzel (3) be van bizonyítva.

IRODALOM

[1] Disquisitiones arithmeticae art. 125 és 129., lásd még Dirichlet–Dedekind, Vorlesungen über Zahlentheorie 4, Auflage (1894), 116. oldal.

[2] A. Brauer, Über den kleinsten quadratischen Nichtrest, Math. Zeitschrift, 33 (1931), 162–176.

[3] J. M. Vinogradoff, On the bound of the least non-residue of k-th powers, Trans. Amer. Math. Soc. 29 (1927), 218–226, lásd még Journal of the Physico–Mathematical Society of Perm. (1919).

[4] H. Davenport and P. Erdős, The distribution of quadratic and higher residues, Publ. Math. Debrecen 2 (1952), 252–265.

[5] D. A. Burgess, The distribution of quadratic residues and non-residues, Mathematika 4 (1957), 106–112.

[6] TURÁN PÁL, „A számelmélet újabb eredményei a Szovjetunióban" Mat. Lapok I. (1950), 243–266.
[7] U. V. LINNIK, A remark on the least quadratic non-residue, Doklady ACAD. Sci. U. S. S. R. (N. S.) **36** (1942), 119–120.
[8] Szóbeli közlés alapján.
[9] Lásd például E. Landau, Zahlentheorie, II. kötet (1927) 178.
[10] PAUL ERDŐS and H. N. SHAPIRO, On the least primitive root of a prime, Pacific Journal of Math. **7** (1957), 861–865.
[11] WANG YUAN: A note on the least primitive root of a prime. Science Record, New Ser. **3** (1959), 174–207.
[12] N. C. ANKENY, Annals of Math. **55** (1952), 5–71.
[13] A. RÉNYI, On the large sieve of Ju. V. Linnik, Compositio Math. **8** (1950), 68–75.
[13] E. C. TITCHMARSH, Rendiconti del Circ. Mat. di Palermo (1930).

ЗАМЕЧАНИЯ ПО ТЕОРИИ ЧИСЕЛ I.

П. Эрдёш

Обозначим через $n_k(p)$ наименьший положительный невычет степени $k \pmod p$. Мирский просил автора найти асимптотическую формулу для $\sum_{p \leqq x} n_k(p)$. Автор доказывает, пользуясь большим решетом Линника, что

$$\sum_{p \leqq x} n_2(p) = (1 + o(1)) \sum_{k=1}^{\infty} \frac{p_k}{2^k} \frac{x}{\log x}$$

где $p_1 < p_2 < \cdots$ последовательность всех простых чисел в натуральном порядке.

Очень вероятен, что $\sum_{p<x} n_k(p) = (1 + o(1)) \frac{c_k x}{\log x}$.

REMARKS ON NUMBER THEORY I.

P. ERDŐS

Denote by $n_k(p)$ the smallest positive k-th power non-residue (mod p). Mirsky asked the author to find an asymptotic formula for $\sum_{p \leqq x} n_k(p)$. The author proves using the large sieve of Linnik that $p_1 < p_2 < \cdots$ are the sequence of consecutive primes

$$\sum_{p \leqq x} n_2(p) = (1 + o(1)) \sum_{k=1}^{\infty} \frac{p_k}{2^k} \frac{x}{\log x}.$$

It is very likely true that $\sum_{p<x} n_k(p) = (1 + o(1)) \frac{c_k x}{\log x}$.