On a classification of primes

By I. KÁTAI in Budapest

1. Let l, D be coprime natural numbers. The letters $p, p_1, \cdots, q, q_1, \cdots$ denote prime numbers. Let $\mathcal{A}_{D,l}$ denote the set of those p for which $q \nmid p+1$, if $q \equiv l \pmod D$. Let $N(x, D, l)$ be the number of the elements of $\mathcal{A}_{D,l}$ which are smaller than x. It seems to be interesting to know whether $N(x, D, l) \to \infty$ for $x \to \infty$ or not. Using the variance-method due to YU. V. LINNIK [1], or the method of C. HOOLEY [2] combined with BOMBIERI's large sieve theorem (see [3]), we deduce the inequality

$$N(x, 4, 3) \gg \frac{x}{(\log x)^4}. \tag{1.1}$$

Sharpening the method of HOOLEY we are also able to prove that

$$N(x, D, l) \gg \frac{x}{(\log x)^4}, \tag{1.2}$$

provided that there exists some Dirichlet character $\chi \pmod D$ such that $\chi(l) = -1$. For the remaining cases we are unable to prove that $N(x, D, l) \to \infty$ for $x \to \infty$.

Furthermore, by SELBERG's sieve method we obtain

$$N(x, D, l) \ll x/(\log x)^{1-1/\varphi(D)}. \tag{1.3}$$

It seems probable that this is the exact order of $N(x, D, l)$.

We shall give a detailed proof of the inequalities (1.1)—(1.2) in another paper. Here we investigate only the special case $l = D-1$, D prime, and one of its applications.

Let $\varphi(n)$ denote the Euler function, and $\sigma(n)$ the sum of the positive divisors of n. Let $\varphi(n) = \varphi_1(n)$, $\sigma(n) = \sigma_1(n)$, $\varphi_k(n) = \varphi(\varphi_{k-1}(n))$, $\sigma_k(n) = \sigma(\sigma_{k-1}(n))$ for all $k \geqq 2$.

Let D be a fixed odd prime. We say, that the prime number q belongs to the rth class, if $\varphi_r(q) \equiv 0 \pmod D$ but $\varphi_k(q) \not\equiv 0 \pmod D$, whenever $k < r$. Let $f(D, r, x)$ denote the number of the primes in the rth class smaller than x. Using the prime-number theorem for arithmetical progressions and the eratosthenian sieve, ERDŐS [4] proved that

$$f(D,1,x)=(1+o(1))\frac{x}{(D-1)\log x};\qquad f(D,2,x)=(1+o(1))\frac{D-2}{D-1}\cdot\frac{x}{\log x}.$$

But he has left open the problem whether $f(D, 3, x)\to\infty$ as $x\to\infty$.

We formulate now analogous questions for $\sigma(n)$ instead of $\varphi(n)$.

We say, that the prime number q belongs to the rth class, if $\sigma_r(q)\equiv 0 \pmod D$ but $\sigma_k(q)\not\equiv 0 \pmod D$ whenever $k<r$. Let $g(D, r, x)$ denote the number of the primes in the rth class smaller than x. Using the same method as ERDŐS, it is easy to see that

$$g(D,1,x)=(1+o(1))\frac{1}{D-1}\frac{x}{\log x};\qquad g(D,2,x)=(1+o(1))\frac{D-2}{D-1}\frac{x}{\log x}.$$

In this paper we shall prove, that $g(D, 3, x)\gg x(\log x)^{-4}$ if $x\to\infty$. The method cannot be applied to the lower estimation of $f(D, 3, x)$.

Theorem. *We have* $$g(D,3,x)\gg\frac{x}{(\log x)^4}.$$

Remark. Sharpening the method we are able to improve this inequality (see [5]).

2. For the proof we need some lemmas.

Lemma 1. (E. BOMBIERI [3])

$$\sum_{D\leqq Y}\max_{\substack{l \pmod D\\ (l,D)=1}}\max_{z\leqq x}\left|\pi(z,D,l)-\frac{\operatorname{li} z}{\varphi(D)}\right|\ll\frac{x}{(\log x)^A},$$

where

$$Y=x^{1/2}(\log x)^{-B},\quad B\geqq 4A+40,$$

A being an arbitrary constant.

Let $\chi(n)$ denote a character $\bmod D$ such that $\chi(-1)=-1$. Let further

$$r(n)=\sum_{d|n}\chi(d)=\prod_{p^\alpha||n}\{1+\chi(p)+\cdots+\chi(p^\alpha)\}.$$

Let

$$K(x)=\sum_{\substack{q\leqq x\\ q\not\equiv -1 \pmod D}} r(q+1)|\mu(q+1)|.$$

Using the method of C. HOOLEY [2] combined with the theorem of BOMBIERI (Lemma 1), we can prove the following

Lemma 2. $K(x)=A_D\operatorname{li}x+O(\operatorname{li}x\cdot(\log\log x)^{-\alpha})$, *where* $\alpha>0$, $A_D\neq 0$ *are suitable constants.*

We shall give a detailed proof of this assertion in another paper.

Lemma 3. *Let $N(k, x)$ denote the number of the couples of primes satisfying the conditions $p+1=kq$, $p \leqq x$. Then*

$$N(k,x) \ll \frac{x}{\varphi(k)\log^2 \frac{x}{k}}.$$

For the proof see PRACHAR [6] p. 51, Theorem 4. 6.

Let

$$M(x,y) = \sum_{n \leqq x}' |r(n)|,$$

where the dash means that we sum over those n all prime divisors of which are smaller than y.

Lemma 4. *We have*

$$M(x,y) < x \exp\left(-\frac{\log_3 y}{\log y}\log x + c\log_2 y + O\left(\frac{\log_2 y}{\log_3 y}\right)\right),$$

when $1 < y(x) < x$; $y(x) \to \infty$ *as* $x \to \infty$; $c = \sqrt{2}\left(1 - \frac{1}{D-1}\right)^{1/2}$.

The proof is similar to the proof of RANKIN's theorem (PRACHAR [6], p. 158) and so we omit it.

Let $f(n)$ be a totally additive arithmetical function defined as follows:

$$f(p) = \begin{cases} 1 & \text{when } \; y < p < x^{1/3} \; \text{ and } \; p \equiv -1 \pmod{D}, \\ 0 & \text{otherwise.} \end{cases}$$

Using BOMBIERI's theorem, we obtain:

Lemma 5. *We have*

$$\sum_{q \leqq x} \{f(q+1) - A_{x,y}\}^2 \ll \operatorname{li} x \cdot A_{x,y},$$

where

$$A_{x,y} = \sum_{\substack{y < p < x^{1/3} \\ p \equiv -1 \pmod{D}}} \frac{1}{p}.$$

Corollary. *If* $\frac{\log x}{\log y} \to \infty$, *then the number of those q for which $f(q+1) = 0$ is at most $o(\operatorname{li} x)$.*

Lemma 6. $\sum_{q \leqq x} |r^2(q+1)| \ll x \log^2 x.$

The proof is simple and can be omitted.

3. Proof of the Theorem

The letters $p, q, Q, p_1, p_2, \dots, q_1, q_2, \dots, Q_1, Q_2, \dots,$ denote prime numbers.

Let $\mathfrak{A}_r$ denote the set of those q which belong to the rth class. It is evident that those q in the sum $K(x)$, for which

$$r(q+1)\,\mu(q+1) \neq 0,$$

are not belonging to the classes $\mathfrak{A}_1, \mathfrak{A}_2$. Indeed, if $r(q+1)\,\mu(q+1)\neq 0$, $q \not\equiv -1 \pmod D$ then

(3.1) $$q+1 = q_1 q_2 \cdots q_r,\ (q_1 < \dots < q_r) \quad \text{and} \quad \chi(q_i) \neq -1,$$

i.e. $q_i+1 \not\equiv 0 \pmod D$.

If for a q, represented in the form (3.1), there exists a Q, such that $Q \equiv -1 \pmod D$ and $\sigma(q+1)=(q_1+1)\cdots(q_r+1)\equiv 0 \pmod Q$, but $[\sigma(q+1)\not\equiv \not\equiv 0$ (mod Q then $q \in \mathfrak{A}_3$.

Let

(3.2) $$z_0 = (\log x)^5,\ z_1 = z_0^{\log_2 x},\ z_2 = x^{1/\log_2 x}.$$

Let S_1 denote the set of those q which are represented in the form (3.1), and for which there exists a prime number Q, $Q > z_0$, $Q \equiv -1 \pmod D$ such that

$$\sigma(q+1) \equiv 0 \pmod{Q^2}.$$

Let S_2 denote the set of those q for which

$$\sigma(q+1) \not\equiv 0 \pmod Q,$$

if $Q > z_0$ and $Q \equiv -1 \pmod D$.

Let

(3.3) $$S_i(x) = \sum_{\substack{q \leq x \\ q \in S_i \\ D \nmid q+1}} |r(q+1)|\,|\mu(q+1)| \qquad (i=1,2),$$

and let

$$A_3(x) = \sum_{\substack{q \leq x \\ q \in \mathfrak{A}_3}} |r(q+1)|\,|\mu(q+1)|.$$

Obviously

(3.4) $$A_3(x) \geqq |K(x)| - |S_1(x)| - |S_2(x)|.$$

Lemma 7. *We have*

(3.5) $$S_1(x) = o(\mathrm{li}\, x),$$

(3.6) $$S_2(x) = o(\mathrm{li}\, x).$$

Proof. Since $|r(m)| \leqq d(m)$, where $d(m)$ denotes the number of divisors of m, so we have $S_1(x) \ll \sum_1 + \sum_2$ with

$$\sum\nolimits_1 = \sum_{\substack{z_0 < Q \leqq x \\ Q \equiv -1 (\mathrm{mod}\ D)}} \sum_{\substack{q_1 \equiv q_2 \equiv -1 (\mathrm{mod}\ Q) \\ q_1, q_2 \leqq x}} d(q_1 q_2 m), \quad \sum\nolimits_2 = \sum_{\substack{z_0 < Q \leqq x \\ Q \equiv -1 (\mathrm{mod}\ D)}} \sum_{\substack{q \equiv -1 (\mathrm{mod}\ Q^2) \\ q \leqq x}} d(qm).$$

We obtain evidently, that

$$\sum\nolimits_1 \ll x \log x \sum_{z_0 < Q \leqq x} \sum_{\substack{q_1 \equiv q_2 \equiv -1 (Q) \\ q_1, q_2 \leqq x}} \frac{1}{q_1 q_2} \ll \frac{x (\log x)^3}{z_0} \ll \frac{x}{\log^2 x}.$$

Similarly, we have

$$\sum\nolimits_2 \ll \sum_{z_0 < Q \leqq x} \frac{x \log^3 x}{Q^2} \ll \frac{x}{\log^2 x}$$

and so (3. 5) is proved.

In order to prove (3. 6), let

$$S_2(x) = S_3(x) + S_4(x),$$

where in $S_3(x)$ we sum over those $q+1$ the greatest prime divisor of which is smaller than z_2, and in $S_4(x)$ over the others.

Using Lemma 4, we easily deduce that

$$S_3(x) \leqq M(x, z_2) \ll \frac{x}{\log^2 x}.$$

We consider now $S_4(x)$. For the q occurring in the sum $S_4(x)$ let $q+1 = A(q)\, B(q)$, where

$$A(q) = \prod_{\substack{p \mid q+1 \\ p \leqq z_1}} p, \quad B(q) = \prod_{\substack{p \mid q+1 \\ p > z_1}} p.$$

Let p^* denote the maximal prime divisor of $q+1$, and write

$$B^*(q) \cdot p^* = B(q), \quad A(q) B^*(q) = k.$$

Since, for a fixed k, by Lemma 3 it follows that

$$\sum_{A(q)B^*(q)=k} r(q+1) \ll |r(k)| N(k, x) \ll \frac{|r(k)|}{\varphi(k)} \frac{x}{\log^2 \frac{x}{k}},$$

so we have

$$S_4(x) \ll \sum_{k \leqq \frac{x}{z_2}} |r(k)| N(k, x) \ll \frac{x (\log_2 x)^2}{\log^2 x} \sum_{k \leqq \frac{x}{z_2}} \frac{|r(k)|}{\varphi(k)} \ll$$

$$\ll \frac{x (\log_2 x)^2}{\log^2 x} \prod_{p \leqq z_1} \left\{1 + \frac{|r(p)|}{p-1}\right\} \cdot \prod_{\substack{z_1 < p \leqq x \\ p \in \mathcal{T}}} \left\{1 + \frac{|r(p)|}{p-1}\right\}.$$

Here $\mathscr{T}$ denotes the set of those p for which $p+1\not\equiv 0 \pmod{Q}$, if $Q\equiv -1 \pmod{D}$ and $Q>z_0$.

Obviously

$$\prod_{p<z_1}\left\{1+\frac{|r(p)|}{p-1}\right\}\ll(\log z_1)^2\ll(\log_2 x)^4.$$

Furthermore, applying Lemma 5 and the Corollary to $y=z_0$, $u\geqq z_1$, we have

$$\log\prod_{\substack{z_1<p\leqq x\\ p\in\mathscr{T}}}\left\{1+\frac{|r(p)|}{p-1}\right\}<2\sum_{2^\nu\leqq\frac{x}{z_1}}\sum_{\substack{2^\nu z_1<p\leqq 2^{\nu+1}z_1\\ p\in\mathscr{T}}}\frac{1}{p}<\varepsilon\log_2 x,$$

whence it follows

$$\prod_{\substack{z_1<p<x\\ p\in\mathscr{T}}}\left\{1+\frac{|r(p)|}{p-1}\right\}\ll(\log x)^\varepsilon.$$

So (3. 6) holds.

Taking into account the inequality (3. 4), from Lemma 2 and Lemma 7 it follows that

$$A_3(x)\gg \operatorname{li} x.$$

Using the Cauchy—Schwartz inequality and Lemma 6, we obtain

$$\frac{x}{\log x}\ll A_3(x)\ll\left\{\sum_{\substack{q\leqq x\\ q\in\mathfrak{A}_3}}1\right\}^{1/2}\left\{\sum_{q\leqq x}|r^2(q+1)|\right\}^{1/2}\ll g(D,3,x)^{1/2}\cdot x^{1/2}\log x.$$

Hence the assertion of the Theorem evidently follows.

Refereces

[1] Ю. В. Линник, Дисперсионный метод в бинарных аддитивных задачах, Изд. Ленинградского Университета, 1961.

[2] C. Hooley, On the representation of numbers as the sum of two squares and a prime, *Acta Math.*, **97** (1957), 189—210.

[3] E. Bombieri, On the large sieve, *Mathematika*, **12** (1965), 201—225.

[4] P. Erdős, Remarks on number theory. II, *Mat. Lapok*, **12** (1961), 161—169 (in Hungarian).

[5] I. Kátai, Statistical theorems for the number of prime factors of integers, *unpublished.*

[6] K. Prachar, *Primzahlverteilung* (Berlin—Heidelberg—Göttingen, 1957).

(Received September 26, 1967)