ACTA ARITHMETICA
LXXXIII.2 (1998)

On the distribution of primitive roots mod p

by

CRISTIAN COBELI (Bucureşti and Rochester, N.Y.) and
ALEXANDRU ZAHARESCU (Bucureşti and Cambridge, Mass.)

1. Introduction. There are many sequences of interest in number theory which are believed to have a Poisson distribution, but in very few cases one is actually able to prove the relevant conjectures. It is our purpose here to expose such a case.

Let p be a large prime number and consider the set of primitive roots mod p with representatives $1 < \gamma_1 < \ldots < \gamma_{\varphi(p-1)} < p$.

In this paper we study the distribution of the number of γ's in the interval $(n, n+t]$, $1 \le n \le p$, where $t \sim \lambda p/\varphi(p-1)$ and λ is a positive constant. We show that if $\varphi(p-1)/p$ is small then the distribution is approximately that of a Poisson variable with parameter λ.

Next we consider the proportion of differences $\gamma_{i+1} - \gamma_i$ which are at least λ times greater than the average, that is,

$$g_p(\lambda) = \frac{\#\{i : 1 \le i \le \varphi(p-1), \gamma_{i+1} - \gamma_i \ge \lambda p/\varphi(p-1)\}}{\varphi(p-1)}, \tag{1}$$

where $\gamma_{\varphi(p-1)+1} = \gamma_1 + p$. A probabilistic reasoning leads one to expect that if $\varphi(p-1)/p$ is small then $g_p(\lambda)$ is close to $e^{-\lambda}$.

We prove that this is true and moreover, for any sequence $\{p_n\}_{n\ge1}$ of primes with $\varphi(p_n - 1)/p_n \to 0$, the sequence $\{g_{p_n}(\lambda)\}_{n\ge1}$ of functions converges to $e^{-\lambda}$ uniformly on compact subsets of $[0, \infty)$.

Since $g_p(\lambda)$ is a step function the condition that $\varphi(p-1)/p$ be small is obviously indispensable in the above statements.

It is interesting to see these results in perspective with the similar problems for quadratic residues (nonresidues). Because the average distance between two quadratic residues is 2, the analogue of $g_p(\lambda)$, which is also a step function, is never close to $e^{-\lambda}$.

To achieve our goal in Section 2 we estimate the number of r-tuples of primitive roots. This is enough to obtain the Poisson distribution in

1991 *Mathematics Subject Classification*: Primary 11A07.

Section 3. An argument inspired from sieve theory is then employed to settle the problem of convergence of $g_p(\lambda)$.

Finally, we mention that all the results we prove refer to the primitive roots in intervals of length greater than $p^{1/2+\delta}$, for any fixed $\delta > 0$. It would be interesting to know if one can obtain the same results for shorter intervals.

2. r-tuples of primitive roots.

In what follows p will be a prime number and $\mathcal{I} = \{M+1, \ldots, M+N\}$ a subset of $\{1, \ldots, p\}$.

For $\mathcal{H} = \{h_1, \ldots, h_r\}$ we denote by $\mathcal{N}(\mathcal{H}) = \mathcal{N}(\mathcal{H}; p, \mathcal{I})$ the number of n's, $n \in \mathcal{I}$, for which all the components of the r-tuple $(n+h_1, \ldots, n+h_r)$ are primitive roots mod p.

More generally, for two disjoint sets $\mathcal{A}$, $\mathcal{B}$ of integers we define $\mathcal{N}(\mathcal{A}, \mathcal{B}) = \mathcal{N}(\mathcal{A}, \mathcal{B}; p, \mathcal{I})$ the number of n's, $n \in \mathcal{I}$, for which $n + a$ is a primitive root for any $a \in \mathcal{A}$, and $n + b$ is not a primitive root for any $b \in \mathcal{B}$. Thus $\mathcal{N}(\mathcal{H}) = \mathcal{N}(\mathcal{H}, \emptyset)$. For p large and $\mathcal{A}, \mathcal{B}$ two sets of integers disjoint mod p, it is reasonable to expect that $\mathcal{N}(\mathcal{A}, \mathcal{B})$ is about $|\mathcal{I}|(\varphi(p-1)/p)^{|\mathcal{A}|}(1-\varphi(p-1)/p)^{|\mathcal{B}|}$. This is confirmed by Theorem 1 below.

The proof goes via counting r-tuples of primitive roots. At this point we follow the approach of Johnsen who investigated this problem in [5]. In order to keep the presentation simple we give only the version which will be needed in what follows. At the same time, we make the necessary changes to obtain the same results in shorter intervals.

Let $\mathcal{H} = \{h_1, \ldots, h_r\}$ be a set of $r \ge 1$ integers, and $\chi_1, \ldots, \chi_r$ Dirichlet characters mod p. Define

$$S(\chi_1, \ldots, \chi_r; \mathcal{H}, \mathcal{I}) = \sum_{n \in \mathcal{I}} \chi_1(n+h_1) \ldots \chi_r(n+h_r).$$

An estimation for $S(\chi_1, \ldots, \chi_r; \mathcal{H}, \mathcal{I})$ is given by the next lemma which may be regarded as a generalized version of the Pólya–Vinogradov inequality.

LEMMA 1. *Let $\mathcal{H} = \{h_1, \ldots, h_r\}$ be a set of distinct integers mod p and $r \ge 1$ Dirichlet characters $\chi_1, \ldots, \chi_r$ not all principal. Then*

$$|S(\chi_1, \ldots, \chi_r; \mathcal{H}, \mathcal{I})| \le 2r\sqrt{p}\log p.$$

Proof. Clearly we may assume that $p \ge 7$ and all characters are nonprincipal. To have $S = S(\chi_1, \ldots, \chi_r; \mathcal{H}, \mathcal{I})$ as a complete sum over all n mod p we write it in terms of Gauss sums:

$$S = \sum_{n=1}^{p} \chi_1(n+h_1) \ldots \chi_r(n+h_r) \sum_{m \in \mathcal{I}} \left[\frac{1}{p} \sum_{k=1}^{p} e\left(k\frac{m-n}{p}\right)\right]$$
$$= \frac{1}{p} \sum_{k=1}^{p} \sum_{m \in \mathcal{I}} e\left(\frac{km}{p}\right) \sum_{n=1}^{p} \chi_1(n+h_1) \ldots \chi_r(n+h_r) e\left(\frac{-kn}{p}\right).$$

Isolating the contribution of the terms in which $k = p$ we have

$$(2)\quad S = \frac{N}{p}\sum_{n=1}^{p}\chi_1(n+h_1)\ldots\chi_r(n+h_r) + \frac{1}{p}\sum_{k=1}^{p-1}\sum_{m\in\mathcal{I}} e\Big(\frac{km}{p}\Big)\sum_{n=1}^{p}\chi_1(n+h_1)\ldots\chi_r(n+h_r)e\Big(\frac{-kn}{p}\Big).$$

A bound for the first sum is given by the following inequality (see Johnsen [5, Lemma 1]):

$$\Big|\sum_{n=1}^{p}\chi_1(n+h_1)\ldots\chi_r(n+h_r)\Big| < (r-1)\sqrt{p}+1.$$

In the other term the first inner sum is a geometric progression and can be calculated explicitly:

$$\sum_{m\in\mathcal{I}} e\Big(\frac{km}{p}\Big) = \frac{e\big(k\frac{M}{p}\big) - e\big(k\frac{M+N+1}{p}\big)}{e\big(\frac{k}{p}\big)-1}.$$

Here the numerator has modulus at most 2, while the modulus of the denominator is $2|\sin(k\pi/p)|$. Hence

$$\Big|\sum_{m\in\mathcal{I}} e\Big(\frac{km}{p}\Big)\Big| \le \Big|\sin\frac{\pi k}{p}\Big|^{-1} \le \Big(2\Big\|\frac{k}{p}\Big\|\Big)^{-1}$$

where $\|\cdot\|$ is the distance to the nearest integer.

To bound the most inner sum in the second line of (2) let χ be a generator of the group of Dirichlet characters mod p. Then $\chi_1(n+h_1)\ldots\chi_r(n+h_r) = \chi(R(n))$, where $R(n) = \prod_{j=1}^{r}(n+h_j)^{\alpha_j}$, and for any $j_1,\ldots,j_r$, $\chi_j = \chi^{\alpha_j}$. Then Weil's estimate (see [8]) gives

$$\Big|\sum_{n=1}^{p}\chi_1(n+h_1)\ldots\chi_r(n+h_r)e\Big(\frac{-kn}{p}\Big)\Big| = \Big|\sum_{n=1}^{p}\chi(R(n))e\Big(\frac{-kn}{p}\Big)\Big| \le r\sqrt{p}.$$

On combining all these, we deduce

$$\begin{aligned}|S(\chi_1,\ldots,\chi_r;\mathcal{H},\mathcal{I})| &\le \frac{N}{p}[(r-1)\sqrt{p}+1] + \frac{1}{p}\sum_{k=1}^{p-1}\frac{1}{2\|k/p\|}r\sqrt{p}\\ &\le \frac{rN}{\sqrt{p}} + r\sqrt{p}\sum_{k=1}^{(p-1)/2}\frac{1}{k} \le 2r\sqrt{p}\log p,\end{aligned}$$

which gives the stated result.

Now we introduce the following characteristic function:

$$(3)\qquad \delta(n) = \begin{cases} 1 & \text{if } n \text{ is a primitive root mod } p,\\ 0 & \text{otherwise.}\end{cases}$$

Similarly, for any integer k, we define

$$\delta_k(n)=\begin{cases}1 & \text{if } n \text{ is a } k\text{-power mod } p,\\ 0 & \text{otherwise.}\end{cases} \tag{4}$$

Obviously, for any $n \bmod p$, $\delta_k(n)=\delta_{(k,p-1)}(n)$, where $(k,p-1)$ is the greatest common divisor of k and $p-1$.

Since $\delta_k(n)=1$ is equivalent with $k \mid \frac{p-1}{\operatorname{ord} n}$ and

$$\sum_{k\mid n}\mu(k)=\begin{cases}1 & \text{if } n=1,\\ 0 & \text{otherwise,}\end{cases}$$

it follows that

$$\delta(n)=\sum_{k\mid p-1}\mu(k)\delta_k(n). \tag{5}$$

On the other hand, if $k \mid p-1$ then there are exactly k Dirichlet characters mod p with $\chi^k=\chi_0$, where χ_0 is the principal character. This implies that

$$\delta_k(n)=\frac{1}{k}\sum_{\chi^k=\chi_0}\chi(n).$$

Inserting this on the right side of (5) we obtain

$$\delta(n)=\sum_{k\mid p-1}\frac{\mu(k)}{k}\sum_{\chi^k=\chi_0}\chi(n). \tag{6}$$

Now we prove the following:

Theorem 1. *Let $\mathcal{A}$, $\mathcal{B}$ be two sets of integers distinct mod p. Then*

$$\left|\mathcal{N}(\mathcal{A},\mathcal{B})-|\mathcal{I}|\left(\frac{\varphi(p-1)}{p}\right)^{|\mathcal{A}|}\left(1-\frac{\varphi(p-1)}{p}\right)^{|\mathcal{B}|}\right| \le 2^{|\mathcal{B}|+1}|\mathcal{A}\cup\mathcal{B}|\sqrt{p}(\log p)(\sigma_0(p-1))^{|\mathcal{A}\cup\mathcal{B}|}.$$

Here $\sigma_0(p-1)$ is the number of divisors of $p-1$.

Proof. We begin with the case $\mathcal{B}=\emptyset$. Then $\mathcal{A}$ is not empty. Set $s=|\mathcal{A}|$. By (6) we have

$$\mathcal{N}(\mathcal{A})=\sum_{n\in\mathcal{I}}\prod_{a\in\mathcal{A}}\delta(n+a)=\sum_{n\in\mathcal{I}}\prod_{a\in\mathcal{A}}\Big[\sum_{k\mid p-1}\frac{\mu(k)}{k}\sum_{\chi^k=\chi_0}\chi(n+a)\Big].$$

Inverting the order of summation, the above is

$$\mathcal{N}(\mathcal{A})=\sum_{k_1\mid p-1}\cdots\sum_{k_s\mid p-1}\frac{\mu(k_1)\ldots\mu(k_s)}{k_1\ldots k_s} \times\sum_{\chi_1^{k_1}=\chi_0}\cdots\sum_{\chi_s^{k_s}=\chi_0}S(\chi_1,\ldots,\chi_s;\mathcal{A},\mathcal{I}).$$

Here the terms with $\chi_j = \chi_0$ for $j = 1, \ldots, s$ have the main contribution. This is equal to

$$N \sum_{k_1 | p-1} \frac{\mu(k_1)}{k_1} \cdots \sum_{k_s | p-1} \frac{\mu(k_s)}{k_s} = N\left(\frac{\varphi(p-1)}{p-1}\right)^s$$
$$= N\left(\frac{\varphi(p-1)}{p}\right)^s \left[1 + O\left(\frac{s}{p}\right)\right].$$

Since all the remaining terms contain at least one nonprincipal character we can apply Lemma 1 to estimate them. The absolute value of their sum is

$$\leq \sum_{k_1|p-1} \cdots \sum_{k_s|p-1} \frac{1}{k_1 \ldots k_s} \sum_{\chi_1^{k_1}=\chi_0} \cdots \sum_{\chi_s^{k_s}=\chi_0} 2s\sqrt{p}\log p$$
$$= 2s\sqrt{p}(\log p) \sum_{k_1|p-1} \cdots \sum_{k_s|p-1} \frac{1}{k_1 \ldots k_s} k_1 \ldots k_s$$
$$= 2s\sqrt{p}(\log p)(\sigma_0(p-1))^s.$$

This concludes the proof in the case $\mathcal{B} = \emptyset$.

Now we take a general $\mathcal{B}$. We write $\mathcal{N}(\mathcal{A},\mathcal{B})$ using the characteristic function $\delta(n)$ and change the order of summation to obtain

$$(7)\quad \mathcal{N}(\mathcal{A},\mathcal{B}) = \sum_{n\in\mathcal{I}} \prod_{a\in\mathcal{A}} \delta(n+a) \prod_{b\in\mathcal{B}} [1 - \delta(n+b)]$$
$$= \sum_{n\in\mathcal{I}} \prod_{a\in\mathcal{A}} \delta(n+a) \sum_{\mathcal{C}\subset\mathcal{B}} (-1)^{|\mathcal{C}|} \prod_{c\in\mathcal{C}} \delta(n+c)$$
$$= \sum_{\mathcal{C}\subset\mathcal{B}} (-1)^{|\mathcal{C}|} \sum_{n\in\mathcal{I}} \prod_{d\in\mathcal{A}\cup\mathcal{C}} \delta(n+d) = \sum_{\mathcal{C}\subset\mathcal{B}} (-1)^{|\mathcal{C}|} \mathcal{N}(\mathcal{A}\cup\mathcal{C}).$$

From the first part of the proof it follows that

$$\mathcal{N}(\mathcal{A}\cup\mathcal{C}) = N\left(\frac{\varphi(p-1)}{p}\right)^{|\mathcal{A}\cup\mathcal{C}|} + 2\theta_{\mathcal{C}}|\mathcal{A}\cup\mathcal{C}|\sqrt{p}(\log p)(\sigma_0(p-1))^{|\mathcal{A}\cup\mathcal{C}|},$$

where $\theta_{\mathcal{C}}$'s are some real numbers with $|\theta_{\mathcal{C}}| \leq 1$. The theorem follows by inserting this in (7).

Let us remark that in Theorem 1 the dependence is only on the length of $\mathcal{I}$ and not on its position in $[1,p]$. Although we expect Theorems 2, 3 and 4 below to be true for intervals as short as p^{δ}, for any constant $\delta > 0$, in order to obtain nontrivial results, from now on we will consider only intervals $\mathcal{I}$ with lengths greater than $p^{1/2+\delta}$.

We note in passing that one has asymptotical results for the number of primitive roots in shorter intervals $\mathcal{I}$ of length $> p^{1/4+\delta}$ (see Burgess [1]). The same phenomenon appears more generally in the case of r-tuples of primitive roots but it seems to vanish when r goes to infinity. This explains why we are not able to use Burgess' ideas to improve on the exponent $1/2$ for $|\mathcal{I}|$ in our results.

For our purpose it is also convenient to express Theorem 1 in a different form transferring the influence of the Euler function and the divisor function on the error term. The size of the divisor function is given by $\sigma_0(n) = O_\delta(n^{(\delta+\log 2)/\log\log n})$ (see Ramanujan [6]). The Euler function is bounded by

$$\phi(n) \geq e^{-\gamma} \frac{n}{\log\log n + \dfrac{5}{2e^{\gamma}\log\log n}},$$

where γ is the Euler constant (see Rosser and Schoenfeld [7]). We also note that $\varphi(p-1)/p \leq 1/2$. Thus we obtain the following:

Corollary 1. *Let $\delta > 0$ be a real number. Assume that $|\mathcal{I}| \geq p^{1/2+2\delta}$ and $\mathcal{A}$, $\mathcal{B}$ are disjoint sets mod p with $1 \leq |\mathcal{A} \cup \mathcal{B}| < \delta \log\log p$. Then*

$$\mathcal{N}(\mathcal{A},\mathcal{B}) = |\mathcal{I}| \left(\frac{\varphi(p-1)}{p}\right)^{|\mathcal{A}|} \left(1 - \frac{\varphi(p-1)}{p}\right)^{|\mathcal{B}|} [1 + O_\delta(p^{-\delta/2})].$$

It would be interesting to know how much one can increase $|\mathcal{A}\cup\mathcal{B}|$ in the statement of Corollary 1. We expect that this result holds true as long as $|\mathcal{I}|(\varphi(p-1)/p)^{|\mathcal{A}|}(1-\varphi(p-1)/p)^{|\mathcal{B}|} > p^\delta$. We note that $|\mathcal{A}|$ cannot be taken to be larger than $\log p$, even if $|\mathcal{I}| = p$ and $\mathcal{B} = \emptyset$. Moreover, there are infinitely many primes p for which $|\mathcal{A}|$ cannot be larger than $(\log p)/\log\log\log p$.

3. The Poisson distribution of primitive roots. We now consider the random variable given by the number of primitive roots mod p in $(n, n+t]$ and calculate the distribution of its restriction to our interval $\mathcal{I}$. Thus for $t \geq 1$ and a nonnegative integer k let us define $P_k(t) = P_k(t; p, \mathcal{I})$ to be the proportion of integers $n \in \mathcal{I}$ for which the interval $(n, n+t]$ contains exactly k primitive roots mod p.

Since $P_k(t) = 0$ for $k > t$, in the following we will assume that $k \leq t$.

There are different ways to proceed in the calculation of $P_k(t)$. One of them is to find the moments of the random variable. This method was used for example by Gallagher [2], who studied the distribution of primes in short intervals under the r-tuple conjecture for prime numbers. Although we can follow the same steps, in our case with Corollary 1 at hand we will proceed as follows.

Clearly we have

$$P_k(t) = \frac{1}{|\mathcal{I}|} \sum_{\substack{\mathcal{C}\subset\{1,\ldots,[t]\} \\ |\mathcal{C}|=k}} \mathcal{N}(\mathcal{C}, \overline{\mathcal{C}}), \tag{8}$$

where $\overline{\mathcal{C}}$ is the set of integers from $[1, t]$ which are not in $\mathcal{C}$.

Suppose that $\delta > 0$ is a fixed real number. Then if $|\mathcal{I}| \ge p^{1/2+2\delta}$ and $k \le t < \delta \log\log p$, by Corollary 1 we have

$$\text{(9)}\quad P_k(t) = \sum_{\substack{\mathcal{C}\subset\{1,\ldots,[t]\}\\ |\mathcal{C}|=k}} \left(\frac{\varphi(p-1)}{p}\right)^{|\mathcal{C}|} \left(1-\frac{\varphi(p-1)}{p}\right)^{|\bar{\mathcal{C}}|} [1+O_\delta(p^{-\delta/2})]$$
$$= \binom{[t]}{k} \left(\frac{\varphi(p-1)}{p}\right)^{k} \left(1-\frac{\varphi(p-1)}{p}\right)^{[t]-k} [1+O_\delta(p^{-\delta/2})].$$

Suppose now that p goes to infinity through a sequence of primes with the property that $\varphi(p-1)/p$ has limit zero, while $\lambda = t\varphi(p-1)/p$ remains constant. This shows that asymptotically the probability distribution of the random variable defined above is that of Poisson with parameter λ, that is,

$$P_k(t) \sim e^{-\lambda}\frac{\lambda^k}{k!}$$

for any nonnegative integer k. More precisely, taking into account the error term we obtain

THEOREM 2. *Let k be a nonnegative integer, $\delta > 0$ and $1 \le t \le \delta \log\log p$ be real numbers. Set $\lambda = t\varphi(p-1)/p$ and suppose $|\mathcal{I}| \ge p^{1/2+2\delta}$. Then*

$$P_k(t) = e^{-\lambda}\frac{\lambda^k}{k!} e^{O((1+k+\lambda)\varphi(p-1)/p)} \left[1 + O\left(\frac{k^2}{\lambda}\cdot\frac{\varphi(p-1)}{p}\right)\right][1+O_\delta(p^{-\delta/2})].$$

Next consider the question of how far an arbitrary $n \in \mathcal{I}$ is to the next primitive root. Let $D(n)$ be the random variable denoting this distance. Clearly, there are no primitive roots in $(n, n+t]$ if and only if $D(n) > t$. Then Theorem 2 for $k = 0$ shows that $D(n)$ is asymptotically exponentially distributed. We obtain

COROLLARY 2. *Denote by $P_{\mathcal{I}}(D > t)$ the probability that $D(n) > t$. Then, under the hypothesis of Theorem 2,*

$$P_{\mathcal{I}}(D > t) = e^{-\lambda} e^{O((1+\lambda)\varphi(p-1)/p)}[1+O_\delta(p^{-\delta/2})].$$

4. The distribution of the differences between consecutive primitive roots. For any real number $\lambda > 0$ denote by $g(\lambda) = g(\lambda; p, \mathcal{I})$ the proportion of differences between consecutive primitive roots in $\mathcal{I}$ which are at least λ times greater than the average $p/\varphi(p-1)$.

Since by Corollary 1 the number of primitive roots in $\mathcal{I}$ is equal to $|\mathcal{I}|(\varphi(p-1)/p)[1+O_\delta(p^{-\delta/2})]$ we have

$$\text{(10)}\qquad g(\lambda) = \frac{pG(\lambda)}{|\mathcal{I}|\varphi(p-1)}[1+O_\delta(p^{-\delta/2})]$$

where $G(\lambda)$ denotes the number of $\gamma_i \in \mathcal{I}$ for which $\gamma_{i+1} - \gamma_i \ge \lambda p/\varphi(p-1)$.

The usual way to get information about $G(\lambda)$ is via estimates for the number of r-tuples of elements from the given sequence. For the general connections, as well as for the treatment of some particular sequences see Hooley [4]. Here we will use a simple relation between $G(\lambda)$ and the quantities $P_k(t)$ from Theorem 2 for which we already have an estimate. One verifies that

$$G(\lambda) = |\mathcal{I}|(P_0(\lceil t\rceil - 1) - P_0(\lceil t\rceil)) \tag{11}$$

for any $\lambda > 0$ and $t = \lambda p/\varphi(p-1)$. Here $\lceil t\rceil$ denotes the smallest integer greater than or equal to t.

On combining (9)–(11), for $1 \le t \le \delta \log\log p$ we deduce

$$\begin{aligned} g(\lambda) &= \frac{p}{\varphi(p-1)}(P_0(\lceil t\rceil - 1) - P_0(\lceil t\rceil))[1 + O_\delta(p^{-\delta/2})] \\ &= \frac{p}{\varphi(p-1)}\left[\left(1 - \frac{\varphi(p-1)}{p}\right)^{\lceil t\rceil - 1} - \left(1 - \frac{\varphi(p-1)}{p}\right)^{\lceil t\rceil}\right][1 + O_\delta(p^{-\delta/2})] \\ &= \left(1 - \frac{\varphi(p-1)}{p}\right)^{\lceil t\rceil - 1}[1 + O_\delta(p^{-\delta/2})]. \end{aligned}$$

For $\varphi(p-1)/p \le \lambda \le \delta(\varphi(p-1)/p)\log\log p$ this implies

$$g(\lambda) = e^{-\lambda + O((1+\lambda)\varphi(p-1)/p)}[1 + O_\delta(p^{-\delta/2})]. \tag{12}$$

Now suppose $\{p_n\}_{n\ge1}$ is a sequence of primes with $\varphi(p_n - 1)/p_n \to 0$. We want to show that the sequence $\{g_{p_n}(\lambda)\}_{n\ge1}$ of functions converges to $e^{-\lambda}$ uniformly on compact subsets of $[0,\infty)$.

The relation (12) implies that this is true provided $1 \le \lambda p_n/\varphi(p_n - 1) \le \delta \log\log p_n$ for n sufficiently large.

The first inequality above is satisfied because $\lambda > 0$ is fixed. However, there are sequences of primes for which the second inequality fails if λ is large enough.

Since Corollary 1 is not strong enough for our purpose we appeal directly to Theorem 1. Proceeding as above we find that our problem would be solved if the following weaker inequality holds for n sufficiently large:

$$\lambda < 2\delta\frac{\varphi(p_n - 1)}{p_n}\cdot\frac{\log p_n}{\log\sigma_0(p_n - 1)}. \tag{13}$$

This inequality is not always true either. What happens is that there are large primes p for which both bounds for $\varphi(p-1)$ and $\sigma_0(p-1)$ used before are simultaneously essentially best possible.

Indeed, the constant $\log 2$ in Ramanujan's bound for $\sigma_0(n)$ is attained for the sequence $\{n_j\}_{j\geq 1}$ given by

$$n_j = \prod_{\substack{q<j \\ q \text{ prime}}} q.$$

On the other hand, for the same numbers n_j the bound provided by Rosser and Schoenfeld is also close to an equality. Now, for large j we know from Linnik's Theorem that there are primes $p_j < n_j^L$ such that n_j divides $p_j - 1$, where L is a positive absolute constant. Then it is easy to see that for such sequences of primes p_j the inequality (13) is false if λ is large in terms of L and δ. With the bound 5.5 for Linnik's constant provided by Heath-Brown [3], we find that even in the most fortunate case when $\mathcal{I} = \{1, \ldots, p\}$, (13) fails for $\lambda > 1.95$.

In order to overcome this difficulty, we would need to have in Corollary 1 asymptotical results for larger sets $\mathcal{A}$, $\mathcal{B}$.

Looking for an improvement we see that formula (7) is not satisfactory because it contains too many terms. In such a situation techniques inspired from sieve theory prove to be very helpful.

In (7) we restrict the range of summation to the subsets $\mathcal{C}$ having at most $2r$ elements, where $r < |\mathcal{B}|/4$ is a parameter to be chosen later. An argument familiar from Brun's sieve method yields

$$\sum_{n\in\mathcal{I}} \prod_{a\in\mathcal{A}} \delta(n+a) \sum_{\substack{\mathcal{C}\subset\mathcal{B} \\ |\mathcal{C}|\leq 2r-1}} (-1)^{|\mathcal{C}|} \prod_{c\in\mathcal{C}} \delta(n+c) \leq \mathcal{N}(\mathcal{A},\mathcal{B})$$
$$\leq \sum_{n\in\mathcal{I}} \prod_{a\in\mathcal{A}} \delta(n+a) \sum_{\substack{\mathcal{C}\subset\mathcal{B} \\ |\mathcal{C}|\leq 2r}} (-1)^{|\mathcal{C}|} \prod_{c\in\mathcal{C}} \delta(n+c).$$

From this we obtain

$$\sum_{\substack{\mathcal{C}\subset\mathcal{B} \\ |\mathcal{C}|\leq 2r-1}} (-1)^{|\mathcal{C}|} \mathcal{N}(\mathcal{A}\cup\mathcal{C}) \leq \mathcal{N}(\mathcal{A},\mathcal{B}) \leq \sum_{\substack{\mathcal{C}\subset\mathcal{B} \\ |\mathcal{C}|\leq 2r}} (-1)^{|\mathcal{C}|} \mathcal{N}(\mathcal{A}\cup\mathcal{C}). \tag{14}$$

Now by Theorem 1 the left hand side of (14) equals

$$\sum_{\substack{\mathcal{C}\subset\mathcal{B} \\ |\mathcal{C}|\leq 2r-1}} (-1)^{|\mathcal{C}|} |\mathcal{I}| \left(\frac{\varphi(p-1)}{p}\right)^{|\mathcal{A}\cup\mathcal{C}|}$$
$$+ O\left[r\binom{|\mathcal{B}|}{2r}(|\mathcal{A}|+2r)\sqrt{p}(\log p)(\sigma_0(p-1))^{|\mathcal{A}|+2r}\right]$$
$$= |\mathcal{I}| \left(\frac{\varphi(p-1)}{p}\right)^{|\mathcal{A}|} \sum_{k\leq 2r-1} (-1)^k \binom{|\mathcal{B}|}{k} \left(\frac{\varphi(p-1)}{p}\right)^k$$

$$+O\left[r\frac{|\mathcal{B}|^{2r}}{(2r)!}(|\mathcal{A}|+2r)\sqrt{p}(\log p)(\sigma_0(p-1))^{|\mathcal{A}|+2r}\right].$$

Similarly the right hand side of (14) is equal to

$$|\mathcal{I}|\left(\frac{\varphi(p-1)}{p}\right)^{|\mathcal{A}|}\sum_{k\le 2r}(-1)^k\binom{|\mathcal{B}|}{k}\left(\frac{\varphi(p-1)}{p}\right)^k$$
$$+O\left[r\frac{|\mathcal{B}|^{2r}}{(2r)!}(|\mathcal{A}|+2r)\sqrt{p}(\log p)(\sigma_0(p-1))^{|\mathcal{A}|+2r}\right].$$

On the other hand, we have

$$\sum_{k\le 2r-1}(-1)^k\binom{|\mathcal{B}|}{k}\left(\frac{\varphi(p-1)}{p}\right)^k\le\left(1-\frac{\varphi(p-1)}{p}\right)^{|\mathcal{B}|}$$
$$\le\sum_{k\le 2r}(-1)^k\binom{|\mathcal{B}|}{k}\left(\frac{\varphi(p-1)}{p}\right)^k.$$

On combining all these it follows that

$$\left|\mathcal{N}(\mathcal{A},\mathcal{B})-|\mathcal{I}|\left(\frac{\varphi(p-1)}{p}\right)^{|\mathcal{A}|}\left(1-\frac{\varphi(p-1)}{p}\right)^{|\mathcal{B}|}\right|$$
$$\le|\mathcal{I}|\left(\frac{\varphi(p-1)}{p}\right)^{|\mathcal{A}|}\binom{|\mathcal{B}|}{2r}\left(\frac{\varphi(p-1)}{p}\right)^{2r}$$
$$+O\left[r\frac{|\mathcal{B}|^{2r}}{(2r)!}(|\mathcal{A}|+2r)\sqrt{p}(\log p)(\sigma_0(p-1))^{|\mathcal{A}|+2r}\right].$$

In what follows we write

$$\eta(\delta,p)=\frac{\delta}{8e^2}\cdot\frac{p}{\varphi(p-1)}\log\log p$$

and assume that $|\mathcal{A}|<(\delta/2)\log\log p$ and $|\mathcal{B}|<\eta(\delta,p)$. To balance the error terms we take $r=(\delta/8)\log\log p$. Now, if $|\mathcal{B}|<(\delta/2)\log\log p$ then we are under the assumption of Corollary 1. If $|\mathcal{B}|\ge(\delta/2)\log\log p$ then we have $r<|\mathcal{B}|/4$ and we can use the above calculation. In both cases the following holds true:

Theorem 3. *Let $\delta>0$ be a real number. Assume that $|\mathcal{I}|\ge p^{1/2+2\delta}$ and $\mathcal{A}$, $\mathcal{B}$ are disjoint sets mod p with $|\mathcal{A}|<(\delta/2)\log\log p$ and $|\mathcal{B}|<\eta(\delta,p)$. Then*

$$\mathcal{N}(\mathcal{A},\mathcal{B})$$
$$=|\mathcal{I}|\left(\frac{\varphi(p-1)}{p}\right)^{|\mathcal{A}|}\left(1-\frac{\varphi(p-1)}{p}\right)^{|\mathcal{B}|}\left[1+O_\delta\left(\left(\frac{|\mathcal{B}|}{e\eta(\delta,p)}\right)^{(\delta/4)\log\log p}\right)\right].$$

From Theorem 3 and (8), for $t < \eta(\delta,p)$ we derive

$$P_0(t) = \left(1 - \frac{\varphi(p-1)}{p}\right)^{[t]}\left[1 + O_\delta\left(\left(\frac{|\mathcal{B}|}{e\eta(\delta,p)}\right)^{(\delta/4)\log\log p}\right)\right].$$

Finally, inserting this on the right side of (11) we conclude with the following theorem which solves the problem raised in the introduction.

THEOREM 4. *Let $\delta > 0$ and $0 \le \lambda \le \frac{\delta}{8e^2}\log\log p$ be real numbers and suppose $|\mathcal{I}| \ge p^{1/2+2\delta}$. Then*

$$g(\lambda; p, \mathcal{I}) = e^{-\lambda + O((1+\lambda)\varphi(p-1)/p)}[1 + O_\delta(e^{-(\delta/8)\log\log p})].$$

References

[1] D. A. Burgess, *On character sums and primitive roots*, Proc. London Math. Soc. (3) 12 (1962), 179–192.

[2] P. X. Gallagher, *On the distribution of primes in short intervals*, Mathematika 23 (1976), 4–9.

[3] D. R. Heath-Brown, *Zero-free regions for Dirichlet L-functions, and the least prime in an arithmetic progression*, Proc. London Math. Soc. (3) 64 (1992), 265–338.

[4] C. Hooley, *On the intervals between consecutive terms of sequences*, in: Proc. Sympos. Pure Math. 24, Amer. Math. Soc., 1973, 129–140.

[5] J. Johnsen, *On the distribution of powers in finite fields*, J. Reine Angew. Math. 253 (1971), 10–19.

[6] S. Ramanujan, *Highly composite numbers*, Proc. London Math. Soc. (2) 14 (1915), 347–409.

[7] B. Rosser and L. Schoenfeld, *Approximate formulas for some functions of prime numbers*, Illinois J. Math. 6 (1962), 64–94.

[8] A. Weil, *On some exponential sums*, Proc. Nat. Acad. Sci. U.S.A. 34 (1948), 204–207.

Institute of Mathematics of
the Romanian Academy
P.O. Box 1-764
70700 Bucureşti, Romania

Department of Mathematics
Massachusetts Institute of Technology
77 Mass. Ave.
Cambridge, Massachusetts 02139
U.S.A.
E-mail: azah@math.mit.edu

Department of Mathematics
University of Rochester
Hylan Building, 915
Rochester, New York 14642
U.S.A.
E-mail: ccobeli@math.rochester.edu

Received on 4.3.1997 (3146)