LEAST TOTIENTS IN ARITHMETIC PROGRESSIONS

JAVIER CILLERUELO AND MOUBARIZ Z. GARAEV

Abstract. Let $N(a,m)$ be the least integer n (if exists) such that $\varphi(n) \equiv a \pmod{m}$. Friedlander and Shparlinski proved that for any $\varepsilon > 0$ there exists $A = A(\varepsilon) > 0$ such that for any positive integer m which has no prime divisors $p < (\log m)^A$ and any integer a with $\gcd(a,m) = 1$, we have the bound $N(a,m) \ll m^{3+\varepsilon}$. In the present paper we improve this bound to $N(a,m) \ll m^{2+\varepsilon}$.

1. Introduction

The distribution properties of the values of Euler's function $\varphi(n)$ in arithmetic progressions have been studied in a series of papers, see for example [1]–[5]. Friedlander and Shparlinski investigated the size of the least integer n, to be denoted by $N(a,m)$, such that

$$\varphi(n) \equiv a \pmod{m}. \tag{1}$$

They proved that if $m = q$ is a prime number, then $N(a,q) \ll q^{5/2+\varepsilon}$, which afterwards was improved by Garaev to $N(a,q) \ll q^{2+\varepsilon}$. In the case of composite modulo m Friedlander and Shparlinski established that for some $A = A(\varepsilon) > 0$ if $(a,m) = 1$ and if m has no prime divisors $p < (\log m)^{A(\varepsilon)}$, then $N(a,m) \ll m^{3+\varepsilon}$. The aim of the present paper is to improve this bound further to $N(a,m) \ll m^{2+\varepsilon}$, which at the same time extends Garaev's bound to this class of composite modulo m.

Theorem 1. *For any $\varepsilon > 0$ there exists $A = A(\varepsilon) > 0$ such that, uniformly for integers $m \geq 1$ which have no prime divisors $p < (\log m)^A$ and a with $(a,m) = 1$, we have the bound*

$$N(a,m) \ll m^{2+\varepsilon}.$$

In the opposite direction, the result of Friedlander and Luca [3] implies that there exists a sequence of arithmetical progressions $a_k \pmod{m_k}$ with $m_k \to \infty$ as $k \to \infty$ such that $N(a_k, m_k)$ exists and

$$\frac{\log N(a_k, m_k)}{\log m_k} \to \infty \quad \text{as} \quad k \to \infty.$$

1991 *Mathematics Subject Classification. 2000 Mathematics Subject Classification:*11B50, 11L40, 11N64.

During the preparation of this paper, J. C. was supported by Grant MTM 2005-04730 of MYCIT.

2. The proof

As in the paper of Friedlander and Shparlinski, we look for a solution of the congruence in question in the form $n = p_1p_2p_3$, where p_j are prime numbers that run through prime numbers of certain disjoint intervals.

Let $k \ge 2$ be a fixed positive integer constant. Let I_1, I_2, I_3 be sets of primes defined as follows:

$$\begin{aligned} I_1 &= \{p: \ 0.5m^{1+1/k} < p \le m^{1+1/k},\ (p-1,m)=1\},\\ I_2 &= \{p: 0.5m < p \le m,\ (p-1,m)=1\},\\ I_3 &= \{p: 0.5m^{1/k} < p \le m^{1/k},\ (p-1,m)=1\}. \end{aligned}$$

The sets I_1, I_2, I_3 are pairwise disjoint for any sufficiently large integer m. We will prove that if m is a large integer with no prime divisors less than $(\log m)^{2(k+3)^2}$ and if $(a,m)=1$, then the congruence

$$(p_1-1)(p_2-1)(p_3-1) \equiv a \pmod m, \quad p_j \in I_j,\ j=1,2,3$$

has solutions. The number J of solutions of this congruence is equal to

$$J = \frac{1}{\varphi(m)} \sum_{\chi} \sum_{p_1,p_2,p_3} \chi\left((p_1-1)(p_2-1)(p_2-1)\right) \overline{\chi}(a)$$

where χ runs through all multiplicative character modulo m and the primes p_1, p_2, p_3 run the sets I_1, I_2, I_3 respectively. Thus

$$J = \frac{|I_1||I_2||I_3|}{\varphi(m)} + \frac{\theta}{\varphi(m)} \sum_{\chi\neq\chi_0} |S_1(\chi)||S_2(\chi)||S_3(\chi)|; \quad |\theta| \le 1, \tag{2}$$

where

$$S_j(\chi) = \sum_{p\in I_j} \chi(p-1),\ j=1,2,3.$$

To prove that $J>0$ it is enough to prove that $\sum_{\chi\neq\chi_0} |S_1(\chi)||S_2(\chi)||S_3(\chi)| < |I_1||I_2||I_3|$.

2.1. **Preliminary lemmas.**

Lemma 2. *The following bounds hold:*

$$|I_1| \gg \frac{m^{1/k}\varphi(m)}{\log m}, \qquad |I_2| \gg \frac{\varphi(m)}{\log m}, \qquad |I_3| \gg \frac{m^{1/k}}{\log m}\frac{\varphi(m)}{m}.$$

Proof. It follows easily from [4, Lemma 4]. □

Lemma 3. *The following bounds hold:*

$$\sum_{\chi} |S_j(\chi)|^2 \ll (\log m)|I_j|^2,\ j=1,2 \tag{3}$$

$$\sum_{\chi} |S_3(\chi)|^{2k} \ll \phi(m)m(\log m)^{k^2-1}. \tag{4}$$

Proof. We easily check that

$$\sum_{\chi} |S_j(\chi)|^2 = \varphi(m) J_j, \qquad j = 1, 2,$$

where J_j is the number of pairs (p, p'), $p, p' \in I_j$ such that $p \equiv p' \pmod m$.

In case of $j = 2$, since $|p - p'| < m$ it implies that $p' = p$ for that pairs, so the number of pairs is exactly $|I_2|$. Lemma 2 gives

$$\sum_{\chi} |S_2(\chi)|^2 = \varphi(m) J_2 = \varphi(m)|I_2| = \frac{\varphi(m)}{|I_2|}|I_2|^2 \ll (\log m)|I_2|^2.$$

In case of $j = 1$, since $|p - p'| < m^{1+1/k}$, for each p, the number of primes p' with $p' \equiv p \pmod m$ is at most $m^{1/k}$. Thus $J_1 \ll m^{1/k}|I_1|$ and again by Lemma 2

$$\sum_{\chi} |S_1(\chi)|^2 \ll \varphi(m) m^{1/k}|I_1| \le \frac{\varphi(m) m^{1/k}}{|I_1|}|I_1|^2 \ll (\log m)|I_1|^2.$$

To prove (4) we observe that

$$\sum_{\chi} |S_3(\chi)|^{2k} = \varphi(m) J_3, \tag{5}$$

where J_3 is the number of $(p_1, \dots, p_k, p'_1, \dots, p'_k)$ with $p_i, p'_i \in I_3$ such that

$$(p_1 - 1) \cdots (p_k - 1) \equiv (p'_1 - 1) \cdots (p'_k - 1) \pmod m.$$

Since both products are less than m, the number of solutions of this congruence is bounded by

$$J_3 \le \sum_{n \le m} \tau_k^2(m), \tag{6}$$

where

$$\tau_k(n) = \#\{(n_1, \dots, n_k) : \ n_1 \cdots n_k = n\}$$

is the generalized divisor function. Now combining the well known inequality

$$\sum_{n \le m} \tau_k^2(n) \ll m(\log m)^{k^2-1}$$

with inequalities (5) and (6), we obtain (4). □

Lemma 4. *If $\chi \ne \chi_0$, then*

$$|S_1(\chi)| \ll (\log m)^{-k^2-6k-3}(\log\log m)|I_1|.$$

Proof. We can write

$$S_1(\chi) = \sum_{p \in I_1} \chi(p-1) = \sum_{0.5 m^{1+1/k} < p \le m^{1+1/k}} \chi(p-1),$$

since $\chi(p-1)=0$ when $(p-1,m)>1$. Then

$$\begin{aligned} |S_1(\chi)| &= \left|\sum_{p\le m^{1+1/k}}\chi(p-1) - \sum_{p\le 0.5m^{1+1/k}}\chi(p-1)\right| \\ &\le \left|\sum_{p\le m^{1+1/k}}\chi(p-1)\right| + \left|\sum_{p\le 0.5m^{1+1/k}}\chi(p-1)\right|. \end{aligned}$$

From Rakhmonov's work [6] it is known that if $\chi\ne\chi_0$ is a multiplicative character modulo m and $(l,m)=1$, then

$$\left|\sum_{p\le x}\chi(p-l)\right| \le x(\log x)^5\tau(q)\left(\sqrt{1/q+q\tau^2(q_1)/x}+x^{-1/6}\tau(q_1)\right),$$

where q is the modulo of the conductor of χ, $q_1=\prod_{p|m,p\nmid q}p$ and τ is the divisor function.

For $x=m^{1+1/k}$ or $x=0.5m^{1+1/k}$ it gives

$$\begin{aligned} \left|\sum_{p\le x}\chi(p-l)\right| &\ll m^{1+1/k}(\log m)^5\frac{\tau(q)}{\sqrt{q}} \\ &+ m^{1/2+1/(2k)}(\log m)^5 q^{1/2}\tau(q_1)\tau(q) \\ &+ m^{(1+1/k)5/6}(\log m)^5\tau(q_1)\tau(q). \end{aligned}$$

Since $q\le m$, $k\ge 2$ and $\tau(q_1)\tau(q)\le\tau(m)\ll m^{1/(4k)}$ we obtain

$$\left|\sum_{p\le x}\chi(p-l)\right| \ll m^{1+1/k}(\log m)^5\frac{\tau(q)}{\sqrt{q}} + m^{1+3/(4k)}(\log m)^5.$$

The maximum value of $\frac{\tau(q)}{\sqrt{q}}$ holds when q is the least prime divisor of m, which is greater than $(\log m)^{2(k+3)^2}$. Thus

$$\begin{aligned} \left|\sum_{p\le x}\chi(p-l)\right| &\ll m^{1+1/k}(\log m)^{5-(k+3)^2} + m^{1+3/(4k)}(\log m)^5 \\ &\ll \frac{m}{\varphi(m)}(\log m)^{6-(k+3)^2}|I_1|. \end{aligned}$$

Finally we use the known estimate, $\frac{m}{\varphi(m)}\ll\log\log m$. □

2.2. **End of the Proof.** Following the idea of [5], we split the set of nonprincipal characters into two subsets:

$$\mathcal{A}=\{\chi\ne\chi_0:\ |S_3(\chi)|\le|I_3|(\log m)^{-2}\};$$

$$\mathcal{B}=\{\chi\ne\chi_0:\ |S_3(\chi)|>|I_3|(\log m)^{-2}\}.$$

Thus, from (2) we have

$$J = \frac{|I_1||I_2||I_3|}{\varphi(m)} + \frac{\theta}{\varphi(m)}\sum_{\mathcal{A}} + \frac{\theta}{\varphi(m)}\sum_{\mathcal{B}}; \quad |\theta| \le 1, \tag{7}$$

where

$$\sum_{\mathcal{A}} = \sum_{\chi\neq\chi_0} |S_1(\chi)||S_2(\chi)||S_3(\chi)|,$$
$$\sum_{\mathcal{B}} = \sum_{\chi\in\mathcal{B}} |S_1(\chi)||S_2(\chi)||S_3(\chi)|.$$

To estimate $\sum_{\mathcal{A}}$ we observe that

$$\sum_{\mathcal{A}} \le |I_3|(\log m)^{-2}\left(\sum_{\chi}|S_1(\chi)|^2\right)^{1/2}\left(\sum_{\chi}|S_2(\chi)|^2\right)^{1/2}.$$

Using Lemma 3 we get that

$$\sum_{\mathcal{A}} \ll (\log m)^{-1}|I_1||I_2||I_3|. \tag{8}$$

To estimate $\sum_{\mathcal{B}}$, we first note that

$$\sum_{\mathcal{B}} \le |\mathcal{B}|\left(\max_{\chi\neq\chi_0}|S_1(\chi)|\right)|I_2||I_3|.$$

Next we estimate $|\mathcal{B}|$ using Lemma 3:

$$|\mathcal{B}||I_3|^{2k}(\log m)^{-4k} \le \sum_{\chi}|S_3|^{2k} \ll \varphi(m)m(\log m)^{k^2-1}.$$

Thus

$$|\mathcal{B}| \ll (\log m)^{k^2+4k-1}\varphi(m)m\left(\frac{m^{1/k}}{\log m}\frac{\varphi(m)}{m}\right)^{-2k} \ll (\log m)^{k^2+6k-1}\left(\frac{m}{\varphi(m)}\right)^{2k-1}.$$

We use again that $\frac{m}{\varphi(m)} \ll \log\log m$ and Lemma 4 to obtain

$$\begin{aligned}\sum_{\mathcal{B}} &\ll |\mathcal{B}|(\log m)^{-k^2-6k-3}(\log\log m)|I_1||I_2||I_3| \\ &\ll (\log m)^{-4}(\log\log m)^{2k}|I_1||I_2||I_3|.\end{aligned}$$

Inserting this estimate together with (8) into (7), we get that

$$J = \frac{|I_1||I_2||I_3|}{\varphi(m)}\left(1 + O((\log m)^{-1})\right).$$

Thus, we have proved that for m large enough the congruence

$$(p_1-1)(p_2-1)(p_3-1) \equiv a \pmod m$$

has some solution $p_1 \in I_1,\ p_2 \in I_2,\ p_3 \in I_3$. Since, $(p_1-1)(p_2-1)(p_3-1) \le m^{2+2/k}$, we finish the proof of our Theorem.

References

[1] T. Dence and C. Pomerance, *Eulers function in residue classes*, The Ramanujan J. 2 (1998), 720.
[2] K. Ford, S. Konyagin and C. Pomerance, *Residue classes free of values of the Euler function*, in Number Theory in Progress, K. Gyory, H. Iwaniec, and J. Urbanowicz, eds., vol. 2, de Gruyter, Berlin and New York, 1999, 805-812.
[3] J. Friedlander and F. Luca, *Residue Classes Having Tardy Totients*, arXiv: math.NT/0709.3056v1.
[4] J. Friedlander and I. Shparlinski, *Least totient in residue class*, Bull. London Math. Soc. 39 (2007) 425432. Corrigendum in: *L*east totient in residue class, Bull. London Math. Soc. (2008) doi:10.1112/blms/bdn037.
[5] M. Garaev, *A note on the least totient of a residue class*, The Quaterly Journal of Mathematics, doi:10.1093/qmath/han005.
[6] Z. Kh. Rakhmonov, *On the distribution of values of Dirichlet characters and their applications*, Proc. Steklov Inst. Math. 207 (1995) 263-272.

Departamento de Matemáticas, Universidad Autónoma de Madrid, Madrid-28049, Spain

E-mail address: franciscojavier.cilleruelo@uam.es

Instituto de Matemáticas, Universidad Nacional Autónoma de México, Campus Morelia, Apartado Postal 61-3 (Xangari), C.P. 58089, Morelia, Michoacán, México

E-mail address: garaev@matmor.unam.mx