PRODUCT OF PRIMES IN ARITHMETIC PROGRESSIONS

OLIVIER RAMARÉ, PRIYAMVAD SRIVASTAV,
AND WITH AN APPENDIX OF ORIOL SERRA

Abstract. We prove that, for all $q \geq 2$ and for all invertible residue classes a modulo q, there exists a natural number $n \leq (650q)^9$ that is congruent to a modulo q and that is the product of exactly three primes, all of which are below $(650q)^3$. The proof is further supplemented with a self-contained proof of the special case of the Kneser Theorem we use.

1. Introduction and results

Our main result is the following theorem.

Theorem 1.1. *For all $q \geq 2$ and for all invertible residue classes a modulo q, there exists a natural number $n \leq (650q)^9$ that is congruent to a modulo q and that is the product of exactly three primes, all of which are below $(650q)^3$.*

We follow and improve on the approach initiated in [22] where the authors obtained a similar statement, though with $q^{16/3}$ instead of $(650q)^3$. These two authors had sought the simplest argument, and we stay close to this idea. An appendix by Oriol Serra furthermore provides the reader with a simple proof of the special case of Kneser's Theorem that we need, namely with equal summands.

We recall that Xylouris' version of Linnik's Theorem [28] tells us that, for every modulus q and every invertible residue class a modulo q, one can find a prime congruent to a modulo q that is below $q^{5.18}$ *provided* q is large enough. The proof relies on intricate techniques, and though the result is indeed effective, no one has been able to give any explicit version of it. One could hope to relax the condition from being a prime to being a product of two primes, a problem for which our method fails, but again, explicit results seem to be (very) difficult to obtain. A conjecture of P. Erdös, A. Odlyzko and A. Sárközy in [5] predicts that we can find two primes p_1 and p_2 both less than q and such that $p_1 p_2 \equiv a[q]$.

In order to prove Theorem 1.1, we need a (smoothed) version of the Brun-Titchmarsh Theorem for cosets, and this is the main novelty of this paper. This result is of independent interest and here is the theoretical core of our approach.

Theorem 1.2. *Let $x \geq 0$ and $y > 0$. Let $q \geq 1200$ be an integer and Y be another positive integer such that $Y < y/(\sqrt{q}\log q)$. Let $G = (\mathbb{Z}/q\mathbb{Z})^*$ and $H \subseteq G$ be a*

2000 *Mathematics Subject Classification.* Primary: 11N13, 11A41, Secundary: 11N37, 11B13.

Key words and phrases. Primes in arithmetic progressions, Least prime quadratic residue, Linnik's Theorem.

The first and second authors have been partly supported by the Indo-French Centre for the Promotion of Advanced Research – CEFIPRA, project No 5401-1.

subgroup of index Y. Then

$$\sum_{\substack{x<p\leq x+y,\\ p\in uH}} 1 \leq \frac{2\cdot y}{Y\log\frac{y}{Y\sqrt{q}\log q}}\Big(1+\mathcal{O}\Big(1/\log\frac{y}{Y\sqrt{q}\log q}\Big)\Big)$$

for any class u in G.

When x is arbitrary and $y\leq q$, this result does not have any ancestors as far as we know. When x is arbitrary and $y>q$, we can sum the point-wise bound given by the Brun-Titchmarsh inequality (recalled as Lemma 4.3 below) over the relevant coset: our result is better than the final estimate when $Y<\sqrt{q}/\log q$. When $x=0$, several authors among which we cite Y. Motohashi in [**14**], H. Iwaniec in [**10**], or with J. Friedlander in [**6**] and J. Maynard in [**12**] improved on the classical Brun-Titchmarsh inequality, and summing over the classes, these estimates improve on our result provided q and Y are small enough. For instance, when Y is fixed and $q=y^\theta$ (together with $x=0$), the usage of [**10**, Theorem 3] results in a better bound provided that $\theta<9/20=0.45$ while Theorem 1.2 is otherwise superior (if we have not missed any other estimate! It is however sure is that all the previous bounds explode when q gets close to y while ours does not). Our saving comes from the additional summation over the coset. There exists a third range between x arbitrary and $x=0$: when y is a small power of x. Such a range is explored for instance in [**10**, section 6].

Let us now turn to the smoothed version of Theorem 1.2 we need. The smoothing has the effect of removing the $\log q$; the numerical estimates are also sharper.

Definition 1.3. For any function η from $\mathbb{R}$ to $\mathbb{C}$ with compact support and any $y>0$, we define $\pi_\eta(y)=\sum_p\eta(p/y)$ where the variable p ranges over the primes.

Definition 1.4. Let $q>1$ be a positive integer and $G=(\mathbb{Z}/q\mathbb{Z})^*$. Let $H\subseteq G$ be a subgroup, and uH be a coset of H in G. We set

$$\pi_\eta(y;q,uH)=\sum_{p\equiv uH\,(\mathrm{mod}\ q)}\eta(p/y).$$

We select a smoothing η since we need precise numerics and, with our choice, we have Lemma 2.1 at our disposal, in the usage of which we will need Lemma 2.3. We did not investigate from a numerical viewpoint any other smoothings; such an optimisation would at most modify the constant 650 in Theorem 1.6 and not modify the exponent $1/3$ in Theorem 1.1. From now on, the symbol η shall be kept for the function defined by

$$\eta(t)=\begin{cases}2t, & 0\leq t\leq 1/2,\\ 2(1-t), & 1/2\leq t\leq 1,\\ 0, & \text{otherwise.}\end{cases}\tag{1}$$

This function η is supported on $[0,1]$. Here is the general form of the estimate we prove.

Theorem 1.5. *Let $y^2>q\geq 2$ and η be as in (1). Let $Y<y/\sqrt{q}$ and $G=(\mathbb{Z}/q\mathbb{Z})^*$. Let $H\subseteq G$ be a subgroup of index Y. Then*

$$\pi_\eta(y;q,uH)\leq\frac{2\cdot y/2}{Y\log\frac{y}{Y\sqrt{q}}}\Big(1+\mathcal{O}\Big(1/\log\frac{y}{Y\sqrt{q}}\Big)\Big)$$

for any class u in G.

Remark. It may be noted that with this smoothing η, one has

$$\pi_\eta(y) = \sum_p \eta(p/y) \sim \frac{y/2}{\log y}.$$

By following the same proof, we derive a version of the above result that is numerically well tuned for our usage.

Theorem 1.6. *Let $y \geq 650^{15/2}$ and η be as in (1). Let $q \leq y^{1/3}/650$ and $G = (\mathbb{Z}/q\mathbb{Z})^*$. Let $Y \leq (\log y)/(\frac{3}{2}\log 650)$. Let $H \subseteq G$ be a subgroup of index Y. Then*

$$\pi_\eta(y; q, uH) \leq \frac{2.497\, y/2}{Y \log y}$$

for any class u in G.

When $(\log q)/\log y = 1/3 - o(1)$, and say Y is fixed, a usage of (a smoothed form of) the Brun-Titchmarsh inequality, recalled in Lemma 4.3 below (see for instance [**3**, Theorem 4.2] for a smoothed form), would give a constant 3 rather than our 2.497. As a comparison, we mention that:

- The result of Y. Motohashi from [**14**, Theorem 2, (iii)] would yield the (asymptotic) constant $12/5 = 2.4$ instead of our $5/2$. It is also proved in [**14**, Theorem 4] that a constant 2 is achievable under the extended Lindelöf hypothesis.
- The result of H. Iwaniec from [**10**, Theorem 3] would yield the (asymptotic) constant $16/7 = 2.285\cdots$.

Both methods use analytical means and are hard to make explicit.

Notation. Our notation is rather conventional. Let us however specify that we use $f = \mathcal{O}^*(g)$ to says that $|f| \leq g$ and that $\tau(n)$ represents the number of (positive) divisors of n.

Thanks. We thank Professor Ramachandran Balasubramanian for interesting discussions on this topic. The second author, in particular is indebted to him for his useful insights. The referee is to be thanked for his/her very thorough reading of the initial version of this paper and for proposing well thought out modifications.

2. Preliminary results

We start with [**25**, Lemma 3.1].

Lemma 2.1. *Let η be as before and $y > 0$. Then*

$$\sum_n \eta(n/y) = \frac{y}{2} - \frac{2}{y}\left\|\frac{y}{2}\right\|^2$$

where $\|u\|$ is the distance from u to the nearest integer.

Lemma 2.2. *We have*

$$\frac{x}{\log x - 1} \leq \pi(x) \leq \frac{x}{\log x - 1.1},$$

where the lower bound holds for $x \geq 5393$ and the upper bound for $x \geq 4$. Consequently, when $1 \leq q < x$, then

$$\sum_{\substack{p \leq x \\ (p,q)=1}} 1 \geq \frac{x}{\log x},$$

for all $x \geq 5393$.

Proof. The first part is a consequence of [4, Corollary 5.3]. For the second part, just note that $\nu(q)$, the number of primes dividing q is at most $(\log x)/\log 2$. Therefore

$$\sum_{\substack{p\leq x\\(p,q)=1}} 1 = \pi(x) - \nu(q) \geq \frac{x}{\log x - 1} - \frac{\log x}{\log 2}$$

and this latter quantity is at least $x/\log x$ when $x \geq 137$: indeed the derivative of

$$f(x) = \frac{x}{\log x - 1} - \frac{\log x}{\log 2} - \frac{x}{\log x}$$

reads

$$\frac{1}{\log^2 x}\left(1 - \frac{\log x}{(\log x - 1)^2} - \frac{\log^2 x}{2x}\right).$$

When $x \geq 42$, we have $\frac{\log x}{(\log x-1)^2} \leq 1/2$ and $\frac{\log^2 x}{2x} \leq 1/4$. The above derivative is thus non-negative and we check that $f(137) \geq 0$ while $f(136) < 0$. This completes the proof. □

We next recall [25, Lemma 3.4].

Lemma 2.3. *We have*

$$\frac{x^2}{2\log x} + \frac{c_1 x^2}{\log^2 x} \leq \sum_{p\leq x} p \leq \frac{x^2}{2\log x} + \frac{c_2 x^2}{\log^2 x},$$

for all $x \geq 2\cdot 10^7$, *where* $c_1 = 0.239818$ *and* $c_2 = 0.29251$.

Lemma 2.4. *When* $y \geq 16$, *we have*

$$\frac{4}{y-1} - \frac{2}{y - \log 2 - 1.1} + \frac{1}{y - \log 2} + \frac{2c_1}{(y-\log 2)^2} - \frac{2}{y} - \frac{4c_2}{y^2} \geq \frac{1}{y - 0.3}$$

where c_1 *and* c_2 *are taken from Lemma 2.3.*

Proof. First note that the left-hand side minus the right hand side is a rational fraction whose denominator is positive when $y > \log 2 + 1.1$ and whose numerator reads:

$$\begin{aligned}
&(-\log 2 + 0.80956)y^6 + (3(\log 2)^2 - 4.279112\log 2 - 0.4530304)y^5\\
&\quad + (-3(\log 2)^3 + 7.359396(\log 2)^2 + 0.1893132\log 2 - 0.86439892)y^4\\
&+ ((\log 2)^4 - 5.11984(\log 2)^3 + 1.3739172(\log 2)^2 + 4.12985852\log 2 + 0.22783332)y^3\\
&\quad + (1.22996(\log 2)^4 - 2.031252(\log 2)^3 - 5.3316528(\log 2)^2 - 1.00005972\log 2)y^2\\
&\quad\quad + (0.921052(\log 2)^4 + 2.4172052(\log 2)^3 + 1.1583396(\log 2)^2)y\\
&\quad\quad\quad - 0.351012(\log 2)^4 - 0.3861132(\log 2)^3.
\end{aligned}$$

GP/Pari [16] tells us that the largest root of this polynomial is slightly less than 16, hence the lemma. □

Here is the main lemma of this section.

Lemma 2.5. *Let $x \geq 4 \cdot 10^7$. Then*

$$\pi_\eta(x) \geq \frac{x/2}{\log x - 0.3}.$$

Consequently, it follows for any $1 \leq q < x$, that

$$\sum_{(p,q)=1} \eta(p/x) \geq \frac{x/2}{\log x},$$

for all $x \geq 4 \cdot 10^7$.

Proof. We make use of Lemma 2.2 and 2.3. We have

$$\begin{aligned}\sum_p \eta(p/x) &= 2 \sum_{p \leq x/2} \frac{p}{x} + 2 \sum_{x/2 < p \leq x} \left(1 - \frac{p}{x}\right) = 2\pi(x) - 2\pi(x/2) + \frac{2}{x}\left(\sum_{p \leq x/2} p - \sum_{x/2 < p \leq x} p\right) \\ &= 2\pi(x) - 2\pi(x/2) + \frac{2}{x}\left(2\sum_{p \leq x/2} p - \sum_{p \leq x} p\right) \\ &\geq \frac{2x}{\log x - 1} - \frac{x}{\log x/2 - 1.1} + \frac{2}{x}\left(\frac{(x/2)^2}{\log x/2} + \frac{2c_1(x/2)^2}{\log^2 x/2} - \frac{x^2}{2\log x} - \frac{c_2 x^2}{\log^2 x}\right).\end{aligned}$$

By Lemma 2.4 with $y = \log x \geq 16$, we find that

$$\frac{4}{y-1} - \frac{2}{y - \log 2 - 1.1} + \frac{1}{y - \log 2} + \frac{2c_1}{(y - \log 2)^2} - \frac{2}{y} - \frac{4c_2}{y^2} \geq \frac{1}{y - 0.3}$$

from which we deduce that $\sum_p \eta(p/x) \geq \frac{x/2}{\log x - 0.3}$ when $x \geq 9 \cdot 10^6$. This proves our first inequality. For the second part of Lemma 2.5, note that η is bounded by 1, so that

$$\sum_{(p,q)=1} \eta(p/x) = \pi_\eta(x) - \sum_{p|q} \eta(p/x) \geq \pi_\eta(x) - \nu(q) \geq \frac{x/2}{\log x - 0.3} - \frac{\log x}{\log 2} \geq \frac{x/2}{\log x}.$$

This completes the proof. □

3. Character estimates

Here is now a corollary of a theorem from [**11**].

Lemma 3.1. *Let χ be a primitive character modulo q. Then $|\sum_n \chi(n)\eta(n/y)| \leq \sqrt{q}$.*

A somewhat improved version, when $y < q/2^{\nu(q)}$ and $\varphi(q)/q$ is sizeably less than 1, can be found in [**25**, Theorem 2.1] (with bound $(\varphi(q)/q)\sqrt{q} + 2^{\nu(q)-1} y \sqrt{q}^{-1}$) as well as in [**1**, Theorem 2] (the bound is more difficult to state).

In [**22**, Lemma 2,4], we proved very simply a lower bound for $L(1,\chi)$. We could use the same lower bound at the cost of a worse constant in $900q$, but we prefer to present a different and more efficient way.

Lemma 3.2. *When χ is a primitive quadratic character of conductor q. We have*

$$L(1,\chi) \geq 0.96/\sqrt{q}.$$

Proof. The book [**26**] of L. Washington contains a proof of the claimed inequality at the top of page 217 (beware that this number refers to the second edition of this classical monograph) in the proof of Lemma 11.10. □

Numerous improvement are here possible. For instance, the same proof of Washington yields

$$L(1,\chi) \geq 0.96\, h(-\chi(-1)q)/\sqrt{q}$$

where $h(-\chi(-1)q)$ is the cardinality of the class group of $\mathbb{Q}(\sqrt{\chi(-1)q})$. The proof continues by using $h(-\chi(-1)q) \geq 1$ since it is the cardinality of a non-empty set. However Genus theory tells us that $h(-\chi(-1)q) \geq 2^{\omega(q)}$. The reader will find in [19] a purely analytical proof of a similar lower bound when $\chi(-1) = -1$. Furthermore, the hypothesis of Theorem 1.1 ensures us that $q > 1\,856\,563$ (and more!). For quadratic characters χ such that $\chi(-1) = -1$ and $q > 1\,856\,563$, M. Watkins proved in [27] that $h(q) \geq 101$. This is an appreciably better lower bound. Concerning characters with $\chi(-1) = 1$, the fact that the regulator is $\gg \log q$ can be employed to derive an improved lower bound for $L(1,\chi)$. We do not dwell further on these improvements since we do not use them. Note that they are equally independant of a proof of Linnik's Theorem.

Lemma 3.3. *Let $q \geq 3$ and χ be a nontrivial quadratic character modulo q. Then, there is a prime $p \leq 25\, q^2$, such that $\chi(p) = 1$.*

We follow the approach of Lemma 2.5 from Ramaré-Walker, which is actually taken from J. Pintz [17].

Proof. Suppose that $\chi(p) = -1$ for all primes $p \leq x$ and not dividing q. We write $d \mid q^\infty$ to denote that all prime factors of d divide q. Then $(1 * \chi)(n)$ is nonzero only when $n = dm^2$, with $d \mid q^\infty$ and $(m,q) = 1$. Hence

$$\sum_{n\leq x}(1*\chi)(n) = \sum_{d\mid q^\infty}\sum_{\substack{m^2\leq x/d\\(m,q)=1}} 1 \leq \sum_{d\mid q^\infty}\sqrt{\frac{x}{d}} \leq \sqrt{x} f_0(q), \tag{2}$$

where $f_0(q) = \prod_{p\mid q}(1-1/\sqrt{p})^{-1}$. By [22, Lemma 2.1], we have the upper bound $f_0(q) \leq 3.32\sqrt{q}$. We can also write the given sum as

$$\sum_{n\leq x}(1*\chi)(n) = \sum_{d\leq x}\chi(d)\left\lfloor\frac{x}{d}\right\rfloor = x\sum_{d\leq x}\frac{\chi(d)}{d} - \sum_{d\leq x}\chi(d)\left\{\frac{x}{d}\right\} \tag{3}$$

It can be seen that

$$L(1,\chi) = \sum_{d\leq x}\frac{\chi(d)}{d} + \int_x^\infty\left(\sum_{x<d\leq t}\chi(d)\right)\frac{dt}{t^2} = \sum_{d\leq x}\frac{\chi(d)}{d} + \mathcal{O}^*\left(\frac{\varphi(q)}{2x}\right),$$

where we use the bound $|\sum_{n\in I}\chi(n)| \leq \varphi(q)/2$, from [22, Lemma 2.3], for any interval I. For the second term of (3), we use Axer's method from [2]. We have

$$\left|\sum_{d\leq x}\chi(d)\left\{\frac{x}{d}\right\}\right| \leq \sum_{d\leq y}1 + \sum_{m\leq x/y}\left|\sum_{d:\lfloor x/d\rfloor=m}\chi(d)\left\{\frac{x}{d}\right\}\right| \leq y + \frac{\varphi(q)x}{2y} \leq \sqrt{2\varphi(q)x},$$

by choosing $y = \sqrt{\varphi(q)x/2}$. Therefore, this means that $xL(1,\chi) \leq \sqrt{x}f_0(q) + \sqrt{2\varphi(q)} + \varphi(q)/2$. Using the lower bound for $L(1,\chi)$ from Lemma 3.2, we obtain

$$\frac{0.96}{\sqrt{q}} \leq \frac{3.32\sqrt{q}}{\sqrt{x}} + \sqrt{\frac{2\varphi(q)}{x}} + \frac{\varphi(q)}{x}. \tag{4}$$

We further substitute $x = 25q^2$. Our initial hypothesis thus implies that

$$\frac{0.96}{\sqrt{q}} \le \frac{3.32}{\sqrt{25q}} + \sqrt{\frac{2}{25q}} + \frac{1}{25q}$$

which we simplify in

$$\Big(0.96 - \frac{3.32+\sqrt{2}}{\sqrt{25}}\Big)\sqrt{q} \le \frac{1}{25}.$$

This inequality does not hold when $q \ge 4$, getting a contradiction. For $q = 3$, the prime 7 satisfies the required conditions. This completes the proof. □

4. Sieve auxiliaries

We define

$$G(z) = \sum_{\ell \le z} \frac{\mu^2(\ell)}{\varphi(\ell)}. \tag{5}$$

This function is studied in details in [**23**], [**18**] and in [**15**]. We shall however need only a simple lower bound that one may find in [**8**]. We also define the Selberg sieve weight by

$$\lambda_d = \frac{d\mu(d)}{G(z)} \sum_{\substack{\ell \le z \\ \ell \equiv 0 \pmod{d}}} \frac{\mu^2(\ell)}{\varphi(\ell)}. \tag{6}$$

We start with an auxiliary lemma.

Lemma 4.1. *We have*

$$\sum_b \frac{\mu^2(b)\tau(b)}{\varphi(b)\sigma(b)} = \frac{\zeta(2)^2}{\zeta(4)}.$$

Furthermore, for any integer parameter $P \ge 7$, we have

$$A_1 = \sum_b \frac{\mu^2(b)\tau(b)}{\sqrt{b}\varphi(b)} = \zeta(3/2)^2 \prod_{2\le p\le P} \Big(1 + \frac{2p^2 - 3p^{3/2} - \sqrt{p} + 2}{p^{7/2}(p-1)}\Big)\big(1 + \mathcal{O}^*(E_1)\big),$$

where $E_1 + 1 \in [1, \exp(4/(3P^{3/2}))]$. We have $A_1 \le 7.31$. Similarly, we have

$$A_2\zeta(3/2)^{-4} = \sum_b \frac{\mu^2(b)\tau^2(b)}{\sqrt{b}\varphi(b)}\zeta(3/2)^{-4} =$$
$$\prod_{2\le p\le P} \Big(1 + \frac{4p^5 - 10p^{9/2} - 6p^{7/2} + 20p^3 + 4p^2 - 15p^{3/2} - \sqrt{p} + 4}{p^{13/2}(p-1)}\Big)\big(1 + \mathcal{O}^*(E_2)\big).$$

where $E_2 + 1 \in [1, \exp(8/(3P^{3/2}))]$. We have $A_2 \le 28.8$.

Proof. In each of these three cases, we compute the local p-factor. In the first case, we find that it is

$$1 + \frac{2}{p^2-1} = \frac{p^2+1}{p^2-1} = \frac{p^4-1}{(p^2-1)^2}$$

from which our assertion follows readily. In the second case, we find that the local p-factor is

$$1+\frac{2}{\sqrt{p}(p-1)}=\left(1-\frac{1}{p^{3/2}}\right)^{-2}\left(1-\frac{1}{p^{3/2}}\right)^{2}\left(1+\frac{2}{\sqrt{p}(p-1)}\right)$$
$$=\left(1-\frac{1}{p^{3/2}}\right)^{-2}\left(1+\frac{2p^2-3p^{3/2}-\sqrt{p}+2}{p^{7/2}(p-1)}\right).$$

We further check that, when $p\geq 2$,

$$0\leq\frac{2p^2-3p^{3/2}-\sqrt{p}+2}{p^{7/2}(p-1)}\leq\frac{2p^2-2p}{p^{7/2}(p-1)}\leq\frac{2}{p^{5/2}}.$$

We then use $\log(1+x)\leq x$ and a comparison to an integral to get

$$0\leq\log\prod_{p>P}\left(1+\frac{2p^2-3p^{3/2}-\sqrt{p}+2}{p^{7/2}(p-1)}\right)\leq\sum_{p>P}\frac{2}{p^{5/2}}\leq\sum_{n>P}\frac{2}{n^{5/2}}\leq\frac{4}{3P^{3/2}}.$$

We expanded the sum over every integer in the above; the reader who wants to use the fact that the variable p is indeed prime may instead use the more precise Lemma 3.2 from [**20**]. GP/Pari has an efficient and reliable manner of computing $\zeta(3/2)$ and Euler-products as well (simply with the function `prodeuler`). We derive an upper bound for A_1 by using the parameter $P=10^6$. In the third case, we find that the local p-factor is

$$1+\frac{4}{\sqrt{p}(p-1)}=\left(1-\frac{1}{p^{3/2}}\right)^{-4}\left(1-\frac{1}{p^{3/2}}\right)^{4}\left(1+\frac{4}{\sqrt{p}(p-1)}\right).$$

We proceed as before but the computations are more cumbersome and it is better to use some software help. We asked GP/Pari to expand (here q is a symbol for $\sqrt{p}$)

$$(\ (1-1/q^3)^4*(1+4/q/(q^2-1))\ -1\ )*q^{13}*(q^2-1)$$

and deduced from the answer that

$$\left(1-\frac{1}{p^{3/2}}\right)^{4}\left(1+\frac{4}{\sqrt{p}(p-1)}\right)$$
$$=1+\frac{4p^5-10p^{9/2}-6p^{7/2}+20p^3+4p^2-15p^{3/2}-\sqrt{p}+4}{p^{13/2}(p-1)}.$$

We readily check that, when $p\geq 7$, we have

$$0\leq\frac{4p^5-10p^{9/2}-6p^{7/2}+20p^3+4p^2-15p^{3/2}-\sqrt{p}+4}{p^{13/2}(p-1)}\leq\frac{4p^5-4p^4}{p^{13/2}(p-1)}\leq\frac{4}{p^{5/2}}.$$

□

Lemma 4.2. *Let $z>1$ be a real number. We have $G(z)\geq\log z$ and $|\lambda_d|\leq 1$. We also have*

$$\sum_d|\lambda_d|\leq\frac{z}{\log z}\left(\frac{15}{\pi^2}+\frac{30}{\sqrt{z}}\right).$$

Proof. The bound $|\lambda_d| \le 1$ may be found in many exposition of the Selberg sieve. It originates from [9]. From (6), we find that

$$\sum_d |\lambda_d| = \sum_{d\le z} \frac{d\mu^2(d)}{G(z)} \sum_{\substack{l\le z\\ \ell\equiv 0 (\mathrm{mod}\ d)}} \frac{\mu^2(\ell)}{\varphi(\ell)} = \frac{1}{G(z)} \sum_{\ell\le z} \frac{\mu^2(\ell)}{\varphi(\ell)} \sum_{d|\ell} d = \frac{1}{G(z)} \sum_{\ell\le z} \frac{\mu^2(\ell)\sigma(\ell)}{\varphi(\ell)}.$$

Now, write $\frac{\mu^2(\ell)\sigma(\ell)}{\varphi(\ell)} = \sum_{ab=\ell} \mu^2(ab)\tau(b)/\varphi(b)$, so that

$$\sum_{\ell\le z} \frac{\mu^2(\ell)\sigma(\ell)}{\varphi(\ell)} = \sum_{\substack{ab\le z\\ (a,b)=1}} \mu^2(a)\frac{\mu^2(b)\tau(b)}{\varphi(b)} = \sum_{b\le z} \frac{\mu^2(b)\tau(b)}{\varphi(b)} \sum_{\substack{a\le z/b\\ (a,b)=1}} \mu^2(a) \tag{7}$$

Note that

$$\sum_{\substack{m\le y\\ (m,q)=1}} 1 = \sum_{\delta|q} \mu(\delta) \sum_{\substack{m\le y\\ \delta|m}} 1 = \sum_{\delta|q} \mu(\delta)\Big(\frac{y}{\delta} - \frac{1}{2} + \mathcal{O}^*(1/2)\Big) = y\frac{\varphi(q)}{q} + \mathcal{O}^*(2^{\nu(q)-1})$$

since the last equation is true when $q > 1$ and the global expression holds obviously true when $q = 1$. We then find that

$$\begin{aligned}\sum_{\substack{n\le x\\ (n,q)=1}} \mu^2(n) &= \sum_{\substack{d\le\sqrt{x}\\ (d,q)=1}} \mu(d) \sum_{\substack{d^2|n\le x\\ (n,q)=1}} 1 = x\frac{\varphi(q)}{q} \sum_{\substack{d\le\sqrt{x}\\ (d,q)=1}} \frac{\mu(d)}{d^2} + \mathcal{O}^*(2^{\nu(q)-1}\sqrt{x})\\ &= \frac{x}{\zeta(2)}\frac{q}{\sigma(q)} + \mathcal{O}^*((2+2^{\nu(q)-1})\sqrt{x})\end{aligned}$$

Therefore

$$\begin{aligned}\sum_{\ell\le z} \frac{\mu^2(\ell)\sigma(\ell)}{\varphi(\ell)} &\le \sum_{b\le z} \frac{\mu^2(b)\tau(b)}{\varphi(b)} \left(\frac{z}{b\zeta(2)}\frac{b}{\sigma(b)} + (\tfrac{1}{2}\tau(b)+2)\sqrt{\frac{z}{b}}\right)\\ &\le \frac{z}{\zeta(2)} \sum_b \frac{\mu^2(b)\tau(b)}{\varphi(b)\sigma(b)} + \sqrt{z}\left(\sum_b \frac{\mu^2(b)\tau^2(b)}{2\sqrt{b}\varphi(b)} + 2\sum_b \frac{\mu^2(b)\tau(b)}{\sqrt{b}\varphi(b)}\right)\\ &\le \frac{15z}{\pi^2} \ + \ 30\sqrt{z}.\end{aligned}$$

The last inequality comes from Lemma 4.1 since $28.8/2 + 2 \times 7.31 = 29.02 \le 30$. Using the bound $G(z) \ge \log z$, we obtain the desired result. □

A "Brun-Titchmarsh Theorem" is a result that bounds the number of primes in some residue class and in an interval. This is an important topic in the literature, and this kind of results can be proved via the linear sieve or via the Selberg sieve, see [9]. We now state the version we use, namely [13, Theorem 2]. Only the case $x = 0$ is required in our proof.

Lemma 4.3 (Brun-Titchmarsh Theorem)**.** *Let $x \ge 0$ and $y > 0$ be two real numbers. For $1 \le q < y$ and $(a, q) = 1$, we have*

$$\pi(x + y, q, a) - \pi(x, q, a) \le \frac{2y}{\varphi(q)\log(y/q)}.$$

5. Additive combinatorics auxiliaries

Here is the case of Kneser's Theorem we need. We state it with the group operation being denoted by the addition, as is customary, but we will use in the multiplicative group of $\mathbb{Z}/q\mathbb{Z}$. We prove it in the appendix. We recall that, when A and B are two subsets of some abelian group G, we define

$$A+B=\{a+b \ / \ a\in A, b\in B\}.$$

In particular, the number of representations of a given element is not taken into account. The stabilizer, say H, of a subset C of G is defined by

$$H=\{g\in G \ / \ \forall c\in C, g+c\in C\}.$$

This stabilizer is a subgroup of G.

Corollary 5.1. *Let A be a subset of a finite abelian group G. Let H be the stabilizer of $A+A$. Suppose that A meets λ cosets of H. Then*

$$|A+A|\geq (2\lambda-1)|H|.$$

While the previous result is used when the sets we add have a somewhat small cardinality, the next one is tailored for very large sets.

Lemma 5.2. *Let A and B be two subsets of a finite abelian group G satisfying $|A|+|B|>|G|$. Then $A+B=G$.*

Proof. Indeed, let g be some element of G. The set $g-A=\{g-a, a\in A\}$ has $|A|>|G\setminus B|$ elements. It thus contains an element $g-a=b$ of B and this implies that $g=a+b\in A+B$. As g was arbitrary, this proves the lemma. □

6. Proof of Theorems 1.5 and 1.6

Let us first define

$$\gamma(n)=1_{n\equiv uH \pmod q}=\frac{1}{Y}\sum_{\chi \pmod{G/H}}\chi(n\bar{u}). \tag{8}$$

For any character χ on G/H, let χ^* denote the primitive character inducing χ. Following Ramaré & Rumely's trick [21, Pg 414], we consider

$$\gamma^*(n)=\frac{1}{Y}\sum_{\chi \pmod{G/H}}\chi^*(n\bar{u}). \tag{9}$$

This is useful in avoiding the loss occurring due to the imprimitivity of characters in $\gamma(n)$. Let $q(n)$ be the largest divisor of q that is coprime to n. For any $d\mid q$, let $G_d=(\mathbb{Z}/d\mathbb{Z})^*$ and H_d be the projection of the subgroup H in G_d. Then, we have

$$\gamma^*(n)=\frac{\left|G_{q(n)}/H_{q(n)}\right|}{Y}1_{n\equiv uH_{q(n)} \pmod{q(n)}}. \tag{10}$$

Proof. To show this, we write $\chi^* (\mathrm{mod}^*\ G_d/H_d)$, to denote that χ^* is primitive to modulus d and is trivial on H_d. We have

$$\begin{aligned}\gamma^*(n)&=\frac{1}{Y}\sum_{d\mid q(n)}\sum_{\chi^* (\mathrm{mod}^*\ G_d/H_d)}\chi^*(n\bar{u})=\frac{1}{Y}\sum_{\chi \pmod{G_{q(n)}/H_{q(n)}}}\chi(n\bar{u})\\&=\frac{\left|G_{q(n)}/H_{q(n)}\right|}{Y}1_{n\equiv uH_{q(n)} \pmod{q(n)}}.\end{aligned}$$

□

It follows from (10) that

$$\gamma(n) \le \gamma^*(n), \quad \text{for all } n \ge 1.$$

Indeed, when $(n,q) > 1$, we have $\gamma(n) = 0 \le \gamma^*(n)$, while, when $(n,q) = 1$, we have $q(n) = q$ and therefore again $\gamma(n) = \gamma^*(n)$. Let us start the main proof. We first introduce a parameter $z \in [1,y]$ and define $P(z) = \prod_{p\le z} p$. Then

$$\begin{aligned}\pi_\eta(y;q,uH) &= \sum_p \gamma(p)\eta(p/y) \le \sum_{p\le z} \gamma(p)\eta(p/y) + \sum_{(n,P(z))=1} \gamma(n)\eta(n/y)\\ &\le z + \sum_{(n,P(z))=1} \gamma^*(n)\eta(n/y). \end{aligned} \tag{11}$$

We use the Selberg device for bounding above the second sum, simply noting that

$$1_{(n,P(z))=1} \le \Big(\sum_{d|n} \lambda_d\Big)^2 \tag{12}$$

where $(\lambda_d)_d$ is defined in (6). We find that

$$\begin{aligned}\sum_{(n,P(z))=1} \gamma^*(n)\eta(n/y) &\le \sum_n \gamma^*(n)\Big(\sum_{d|n}\lambda_d\Big)^2 \eta(n/y)\\ &\le \sum_{d_1,d_2} \lambda_{d_1}\lambda_{d_2} \sum_{\substack{n,\\ [d_1,d_2]|n}} \gamma^*(n)\eta(n/y)\\ &\le \sum_{d_1,d_2} \lambda_{d_1}\lambda_{d_2} \frac{1}{Y} \sum_{\chi(\mathrm{mod}\ G/H)} \chi^*(\bar u) \sum_{\substack{n,\\ [d_1,d_2]|n}} \chi^*(n)\eta(n/y)\end{aligned}$$

and thus our upper bound reads

$$\sum_{d_1,d_2} \lambda_{d_1}\lambda_{d_2} \frac{1}{Y} \sum_{\chi(\mathrm{mod}\ G/H)} \chi^*(\bar u[d_1,d_2]) \sum_m \chi^*(m)\eta(m[d_1,d_2]/y) = S_0 + S_1 \tag{13}$$

where S_0 is the contribution of the trivial character and S_1 the contribution of the rest of them.

When χ is the trivial character, χ^* is just 1. A classical computation that can be found for instance in [9], equation (1.7) chapter 3, where Σ_1 is defined in (1.1) therein, shows that

$$\sum_{d_1,d_2} \frac{\lambda_{d_1}\lambda_{d_2}}{[d_1,d_2]} = G(z).$$

Therefore, from Lemma 2.1, we have

$$\begin{aligned}S_0 &= \frac{1}{Y}\sum_{d_1,d_2} \lambda_{d_1}\lambda_{d_2} \sum_n \eta(n[d_1,d_2]/y) = \frac{1}{Y}\sum_{d_1,d_2} \lambda_{d_1}\lambda_{d_2}\left(\frac{y}{2[d_1,d_2]} + \mathcal{O}^*(1/2)\right)\\ &= \frac{y/2}{YG(z)} + \mathcal{O}^*\left(\frac{1}{2Y}\left(\sum_d |\lambda_d|\right)^2\right).\end{aligned} \tag{14}$$

Next, we look at the contribution to (13) coming from nontrivial characters modulo q. Note that the characters on G/H can be identified with the set of characters

modulo q that act trivially on H. Let q^* denote the conductor of χ. By Lemma 3.1, we have

$$S_1 \le \frac{1}{Y}\sum_{d_1,d_2}|\lambda_{d_1}||\lambda_{d_2}|\sum_{\substack{\chi \pmod{G/H}\\ \chi\neq\chi_0}}\sqrt{q^*} \le \frac{Y-1}{Y}\sqrt{q}\left(\sum_d|\lambda_d|\right)^2. \tag{15}$$

We have used the bound $q^* \le q$ which is for instance optimal when q is a prime. Therefore, from (11), (14), (15) and the bound $G(z) \ge \log z$ from Lemma 4.2, we get

$$\begin{aligned}\pi_\eta(y;q,uH) &\le z + \frac{y/2}{Y\log z} + \left(\frac{Y-1}{Y}\sqrt{q}+\frac{1}{2Y}\right)\left(\sum_d|\lambda_d|\right)^2\\ &\le z + \frac{y/2}{Y\log z} + \sqrt{q}\frac{z^2}{\log^2 z}\left(\frac{15}{\pi^2}+\frac{30}{\sqrt{z}}\right)^2\end{aligned}$$

where we have used Lemma 4.2 in the last step. To prove Theorem 1.5, we select

$$z = \sqrt{\frac{y}{Y\sqrt{q}}} \tag{16}$$

and the theorem follows readily. To prove Theorem 1.6, let us first assume that we are given a parameter $b \ge 500$ such that

$$y \ge b^{15/2}, \quad Y^{\frac{3}{2}}\log b \le \log y, \quad q \le y^{1/3}/b. \tag{17}$$

We first deduce a more precise inequality from these assumptions:

$$\begin{aligned}\frac{Y\log z}{y/2}\pi_\eta(y;q,uH) &\le 1 + \frac{2zY\log z}{y} + \sqrt{q}\frac{2Yz^2}{y\log z}\left(\frac{15}{\pi^2}+\frac{30}{\sqrt{z}}\right)^2\\ &\le 1 + \frac{2z\log y\log z}{y(3/2)\log b} + \frac{y^{1/6}}{\sqrt{b}}\frac{2z^2\log y}{y(\log z)(3/2)\log b}\left(\frac{15}{\pi^2}+\frac{30}{\sqrt{z}}\right)^2.\end{aligned}$$

We take

$$z = y^a \tag{18}$$

for a parameter $a \in [0.3, 0.5]$ to be chosen. We readily see that the RHS above is a non-increasing function of y and use GP/Pari to find that $b = 650$ ensures that this RHS is ≤ 2.497 (on selecting $a = 0.411063$) while $b = 640$ does not (as shown by a crude plot). This completes the proof of Theorem 1.6.

7. Proof of Theorem 1.2

The proof of Theorem 1.2 follows closely the one of the Theorem 1.5. Let us give a sketch by using the notation of the previous section. We find that

$$\begin{aligned}\sum_{\substack{x<p\le x+y,\\ p\in uH}} 1 = \sum_{x<p\le x+y}\gamma(p) &\le \sum_{p\le z}\gamma(p) + \sum_{\substack{x<p\le x+y,\\ (n,P(z))=1}}\gamma(n)\\ &\le z + \sum_{\substack{x<p\le x+y,\\ (n,P(z))=1}}\gamma^*(n).\end{aligned} \tag{19}$$

The proof then proceeds as before with the obvious changes. For instance, we get

$$S_0 = \frac{y}{YG(z)} + \mathcal{O}^*\left(\frac{1}{Y}\left(\sum_d |\lambda_d|\right)^2\right).$$

The estimate of S_1 does now rely on the Pólya-Vinogradov inequality. We take the explicit form due to D.A. Frolenkov & K. Soundararajan in [7] and which we recall in the next lemma.

Lemma 7.1. *For χ a primitive character to the modulus $q \geq 1200$, we have*

$$\max_{M,N}\Big|\sum_{a=M+1}^{M+N}\chi(a)\Big| \leq \begin{cases} \frac{2}{\pi^2}\sqrt{q}\log q + \sqrt{q} & \text{when } \chi \text{ is even,} \\ \frac{1}{2\pi}\sqrt{q}\log q + \sqrt{q} & \text{when } \chi \text{ is odd.} \end{cases}$$

This latter estimates holds as soon as $q \geq 40$.

It is easy to derive from these inequalities that

$$\forall q \geq 1200, \quad \max_{M,N}\Big|\sum_{a=M+1}^{M+N}\chi(a)\Big| \leq \sqrt{q}\log q.$$

This is enough for our purpose. At the level of equation (15), we replace $\sqrt{q}$ by $\sqrt{q}\log q$. Finally, we choose

$$z = \sqrt{\frac{y}{Y\sqrt{q}\log q}} \tag{20}$$

and the reader will easily complete the proof from then on.

8. Proof of Theorem 1.1

Let $\mathcal{P}(y)$ be the set of primes below y that do not divide q and let A be the image of $\mathcal{P}(y)$ in $G = (\mathbb{Z}/q\mathbb{Z})^*$. We seek to show that $A \cdot A \cdot A = G$. Note that

$$q \leq y^{1/3-1/\delta}, \quad \text{where} \quad \delta = \frac{\log y}{\log 650}. \tag{21}$$

We first obtain a lower bound for $|A|$. From Lemma 2.2 and the Brun-Titchmarsh Theorem, we have

$$\frac{y}{\log y} \leq \sum_{\substack{p\leq y \\ (p,q)=1}} 1 = \sum_{a(\mathrm{mod}\ q)}^{*} \pi(y,q,a) \leq |A|\frac{2y}{\varphi(q)\log(y/q)}.$$

Therefore

$$|A| \geq \frac{\varphi(q)}{2}\left(1 - \frac{\log q}{\log y}\right) \geq \varphi(q)\left(\frac{1}{3} + \frac{1}{2\delta}\right). \tag{22}$$

The combinatorial argument that follows uses in a crucial manner the fact that $|A|/\varphi(q)$ is greater than $1/3 + 1/(2\delta)$; the bound $1/3$ would not be enough.

Now, let H be the stabiliser of $A \cdot A$ in G. Suppose Y is the index of H in G and that A meets λ cosets of H in G. Then, clearly $\lambda \geq \lceil Y\,(1/3 + 1/2\delta)\rceil$. We consider two cases:

Case I. $Y \equiv 0, 1 (\mathrm{mod}\ 3)$.

We note that, in this case $\lambda \geq \lceil Y(1/3 + 1/2\delta) \rceil \geq Y/3 + 2/3$. So, by Corollary 5.1 and (22), we have

$$|A \cdot A| + |A| \geq \left(\frac{2(Y/3 + 2/3) - 1}{Y} + \frac{1}{3} + \frac{1}{2\delta} \right) |G| > |G|.$$

Therefore $A \cdot A \cdot A = G$.

Case II. $Y \equiv 2 (\mathrm{mod}\ 3)$.

First, we consider the case $Y > 2\delta/3$. We have

$$|A \cdot A| + |A| \geq \left(\frac{2Y(1/3 + 1/2\delta) - 1}{Y} + \frac{1}{3} + \frac{1}{2\delta} \right) |G| \geq \left(1 + \frac{3}{2\delta} - \frac{1}{Y} \right) |G| > |G|.$$

We now consider the case $Y \leq 2\delta/3$. We first deal with the case $Y = 2$.

In this case, there is a nontrivial quadratic character $\chi (\mathrm{mod}\ q)$ such that H is the kernel of χ. Note that since $\mathcal{P}(y)$ generates all integers below y that are coprime to q, there is a prime p such that $\chi(p) = -1$, since otherwise $\chi(n) = 1$ for all $n \leq y$ with $(n, q) = 1$ and this would mean that χ is trivial. Also, by Lemma 3.3, there is a prime $p \leq 25q^2 \leq y$, such that $\chi(p) = 1$. Therefore, A meets both the cosets of H i.e., $\lambda = 2$. By Kneser's theorem, we have $A \cdot A = G$ and hence $A \cdot A \cdot A = G$.

It now remains to deal with the case $5 \leq Y \leq 2\delta/3$. It turns out that $2\delta/3 = (\log y)/(3 \log(650)/2)$. This implies that $y \geq 650^{15/2}$. We can thus use Theorem 1.6 together with Lemma 2.5 to obtain a lower bound for λ. We have

$$\frac{y/2}{\log y} \leq \sum_{(p,q)=1} \eta(p/y) = \sum_{u \in A/H} \pi_\eta(y; q, uH) \leq \lambda \frac{2.497\, y/2}{Y \log y}.$$

Therefore,

$$\lambda \geq \left\lceil \frac{Y}{2.497} \right\rceil.$$

If $Y = 5$, then clearly $\lambda \geq 3$ and we have $|A \cdot A| \geq |G|$, and so $A \cdot A \cdot A = G$. So, assume that $8 \leq Y \leq 2\delta/3$. By Kneser's theorem, and (22), we have

$$|A \cdot A| + |A| \geq \left(\frac{\frac{2Y}{2.497} - 1}{Y} + \frac{1}{3} + \frac{1}{2\delta} \right) |G| \geq \left(\frac{2}{2.497} + \frac{1}{3} + \frac{1}{2\delta} - \frac{1}{8} \right) |G| > |G|.$$

This completes the proof of Theorem 1.1.

Appendix A. Kneser for $A = B$ by Oriol Serra

This is a self–contained proof of Kneser's theorem in the symmetric case that relies on the ideas developed in [**24**].

Theorem K. *Let G be an abelian group and $A \subset G$ a finite subset.*
If

$$|A + A| < 2|A| - 1,$$

then $A + A$ is a union of cosets of the stabilizer $H(A + A)$ of $A + A$.

Proof. We may assume that $A + A \neq G$, otherwise the statement is trivial. We may also assume that A generates G. Suppose the result false and choose a counterexample A with minimum cardinality.

Let $U \subset G$ be a minimal subset of G which minimizes

$$|A + X| - |X|,$$

among all finite nonempty subsets $X \subset G$ such that $A + X \neq G$ (A is one of these subsets). By translation we may assume $0 \in A \cap U$.

Claim 1. *U is a proper subgroup of G.*

Proof. It follows from the hypothesis that $|A+U|-|U| \leq |A+A|-|A| < |A|-1$. Therefore $|U| \geq 2$. Let us show that, for every $g \in G$,

$$\text{either } U + g = U \text{ or } (U + g) \cap U = \emptyset. \tag{23}$$

We first note that the operator $\partial_A(X) = |A + X| - |X|$ on the finite subsets of G is submodular: for every pair of finite sets $X, Y \subset G$ we have

$$\partial_A(X \cup Y) + \partial_A(X \cap Y) \leq \partial_A(X) + \partial_A(Y). \tag{24}$$

The inequality follows because every element counted in $\partial_A(X \cup Y)$ is also counted in $\partial_A(X)$ or $\partial_A(Y)$, and if this element is counted in $\partial_A(X \cap Y)$ then it is counted in both $\partial_A(X)$ and $\partial_A(Y)$.

Write $U' = U + g$. Since $\partial_A(\cdot)$ is invariant by translations, (24) yields

$$\partial_A(U \cup U') + \partial_A(U \cap U') \leq 2\partial_A(U). \tag{25}$$

If $U \cap U' \neq \emptyset$ then, by the minimality of $\partial_A(U)$ and U, we have $\partial_A(U \cap U') \geq \partial_A(U)$. Moreover, if there is equality, then $U = U'$ proving the claim.

Suppose on the contrary that $\partial_A(U \cap U') > \partial_A U$. Then (25) yields $\partial_A(U \cup U') < \partial_A U$ which, again by the minimality conditions, imply $A + (U \cup U') = G$. It follows that

$$|G| = |U \cup U'| + \partial_A(U \cup U') < 2|U| + \partial_A(U).$$

But then $U^* = G \setminus (A + U)$ satisfies $|U^*| = |G| - (|U| + \partial_A(U)) < |U|$ and $((-A) + U^*) \setminus U^* \subset (A+U) \setminus U$. Since G is abelian, the map $x \mapsto -x$ is a group automorphism and $-U^*$ is a smaller subset than U with no larger $\partial_A(\cdot)$, a contradiction. □

Let

$$A = \cup_{a \in A}(A \cap (U + a)) = A_0 \cup A_1 \cup \cdots \cup A_t,$$

be the decomposition of A into cosets of U. SInce A generates G we have $t \geq 1$. By translation we may assume that $|A_0| = \min_i |A_i|$ and $0 \in A_0$. We have

$$(t + 1)|U| = \sum_i |A_i + U| = |A + U| < |A| + |U| - 1.$$

It follows that $t|U| < \sum_i |A_i|$ and therefore, by our choice of A_0, $|A_i| + |A_j| > |U|$ for each pair (i, j) except possibly $(0, 0)$. This means that $A_i + A_j$ is a U–coset for all pairs A_i, A_j except possibly for $A_0 + A_0 \subset U$.

Now consider the natural projection $\pi : G \to G/U$. We have

$$|\pi(A) + \pi(A)| \geq 2|\pi(A)| - 1, \tag{26}$$

since otherwise we would find a nontrivial subgroup $\pi(U') < G/U$ as before with

$$|\pi(A) + \pi(U')| < |\pi(A)| + |\pi(U')| - 1,$$

leading to a subgroup $U' < G$ with $|A+U'|-|U'| < |A+U|-|U|$, which contradicts our choice of U. By (26) and the fact that $2(A \setminus A_0)$ is a union of U–cosets, we have

$$2|A| - 1 > |A + A| \geq 2|(A \setminus A_0)| + |A_0 + A_0|,$$

which implies $|A_0 + A_0| < 2|A_0| - 1$. By the minimality of $|A|$, $A_0 + A_0$ is a union of cosets of a proper subgroup $U_0 < U$. Hence $A + A$ is also a union of cosets of U_0. This shows that the stabilizer of $A + A$ is nontrivial. Certainly $A + A = A + A + H$ is a union of cosets of the stabilizer $H = H(A + A)$. □

Corollary 5.1. *Let A be a subset of a finite abelian group G. Let H be the stabilizer subgroup of $A + A$. Suppose that A meets λ cosets of H. Then*

$$|A + A| \geq (2\lambda - 1)|H|.$$

Proof. Let $\pi : G \to G/H$ be the canonical projection. Then $\pi(A)+\pi(A)$ has trivial stabilizer (by maximality of H) and, by Theorem A,

$$|\pi(A) + \pi(A)| \geq 2|\pi(A)| - 1 = 2\lambda - 1.$$

It follows that

$$|A + A| = |H| \cdot |\pi(A) + \pi(A)| \geq (2\lambda - 1)|H|.$$

□

References

[1] Kamil Adamczewski and Enrique Treviño. The smoothed Pólya-Vinogradov inequality. *Integers*, 15:Paper No. A20, 11, 2015.

[2] A. Axer. Über einige Grenzwertsätze. *Wien. Ber.*, 120:1253–1298, 1911.

[3] J. Büthe. A Brun-Titchmarsh inequality for weighted sums over prime numbers. *Acta Arith.*, 166(3):289–299, 2014.

[4] P. Dusart. Estimates of some functions over primes. *Ramanujan J.*, 45(1):227–251, 2018.

[5] P. Erdős, A. M. Odlyzko, and A. Sárközy. On the residues of products of prime numbers. *Period. Math. Hungar.*, 18(3):229–239, 1987.

[6] John Friedlander and Henryk Iwaniec. The Brun-Titchmarsh theorem. In *Analytic number theory (Kyoto, 1996)*, volume 247 of *London Math. Soc. Lecture Note Ser.*, pages 85–93. Cambridge Univ. Press, Cambridge, 1997.

[7] D. A. Frolenkov and K. Soundararajan. A generalization of the Pólya–Vinogradov inequality. *Ramanujan J.*, 31(3):271–279, 2013.

[8] H. Halberstam and H.-E. Richert. *Sieve methods*. Academic Press [A subsidiary of Harcourt Brace Jovanovich, Publishers], London-New York, 1974. London Mathematical Society Monographs, No. 4.

[9] H. Halberstam and H.E. Richert. Mean value theorems for a class of arithmetic functions. *Acta Arith.*, 43:243–256, 1971.

[10] H. Iwaniec. A new form of the error term in the linear sieve. *Acta Arith.*, 37:307–320, 1980.

[11] Mariana Levin, Carl Pomerance, and K. Soundararajan. Fixed points for discrete logarithms. In *Algorithmic number theory*, volume 6197 of *Lecture Notes in Comput. Sci.*, pages 6–15. Springer, Berlin, 2010.

[12] James Maynard. On the Brun-Titchmarsh theorem. *Acta Arith.*, 157(3):249–296, 2013.

[13] H.L. Montgomery and R.C. Vaughan. The large sieve. *Mathematika*, 20(2):119–133, 1973.

[14] Yoichi Motohashi. On some improvements of the Brun-Titchmarsh theorem. *J. Math. Soc. Japan*, 26:306–323, 1974.

[15] Akhilesh P. and O. Ramaré. Explicit averages of non-negative multiplicative functions: going beyond the main term. *Coll. Math.*, 147:275–313, 2017.

[16] The PARI Group, Bordeaux. *PARI/GP, version* `2.7.0`, 2014. `http://pari.math.u-bordeaux.fr/`.

[17] J. Pintz. Elementary methods in the theory of L-functions, VI. On the least prime quadratic residue (modρ). *Acta Arith.*, 32(2):173–178, 1977.

[18] O. Ramaré. On Snirel'man's constant. *Ann. Scu. Norm. Pisa*, 21:645–706, 1995. `http://math.univ-lille1.fr/~ramare/Maths/Article.pdf`.

[19] O. Ramaré. A purely analytical lower bound for $L(1, \chi)$. *Annales Mathématiques Blaise Pascal*, 16(2):259–265, 2009.

[20] O. Ramaré. An explicit density estimate for Dirichlet L-series. *Math. Comp.*, 85(297):335–356, 2016.
[21] O. Ramaré and R. Rumely. Primes in arithmetic progressions. *Math. Comp.*, 65:397–425, 1996.
[22] O. Ramaré and Aled Walker. Products of primes in arithmetic progressions: a footnote in parity breaking. *To appear in J. Number Theory of Bordeaux*, 30(1):219–225, 2018.
[23] H. Riesel and R.C. Vaughan. On sums of primes. *Ark. Mat.*, 21:46–74, 1983.
[24] O. Serra. An isoperimetric method for the small sumset problem. In *Surveys in combinatorics 2005*, volume 327 of *London Math. Soc. Lecture Note Ser.*, pages 119–152. Cambridge Univ. Press, Cambridge, 2005.
[25] Enrique Treviño. The least inert prime in a real quadratic field. *Math. Comp.*, 81(279):1777–1797, 2012.
[26] Lawrence C. Washington. *Introduction to cyclotomic fields*, volume 83 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1997.
[27] M. Watkins. Real zeros of real odd Dirichlet L-functions. *Math. Comp.*, 73(245):415–423, 2004. http://www.math.psu.edu/watkins/papers.html.
[28] Triantafyllos Xylouris. On the least prime in an arithmetic progression and estimates for the zeros of Dirichlet L-functions. *Acta Arith.*, 150(1):65–91, 2011.

Olivier Ramaré, CNRS / Institut de Mathématiques de Marseille, Aix Marseille Université, U.M.R. 7373, Site Sud, Campus de Luminy, Case 907, 13288 MARSEILLE Cedex 9, France
Email address: olivier.ramare@univ-amu.fr
URL: http://iml.univ-mrs.fr/~ramare/

Priyamvad Srivastav, Institute of Mathematical Sciences, Taramani, Chennai, India-600113 and Homi Bhabha National Institute, Training School Complex, Anushakti Nagar, Mumbai, India-400094.
Email address: priyamvads@imsc.res.in

Email address: oriol.serra@upc.edu

Oriol Serra, Universitat Politècnica de Catalunya, C. Pau Gargallo, 14. 08028 Barcelona, Spain