Product of three primes in large arithmetic progressions

Ramachandran Balasubramanian, Olivier Ramaré, Priyamvad Srivastav

1

a

Product of three primes in large arithmetic progressions

Ramachandran Balasubramanian

Institute of Mathematical Sciences, Taramani Chennai India-600113
and Homi Bhabha National Institute, Training School Complex
Anushakti Nagar, Mumbai, India-400094.
balu@imsc.res.in

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
olivier.ramare@univ-amu.fr

Priyamvad Srivastav

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

Received (Day Month Year)
Accepted (Day Month Year)

For any $\epsilon > 0$, there exists $q_0(\epsilon)$ such for any $q \geq q_0(\epsilon)$ and any invertible residue class a modulo q, there exists a natural number that is congruent to a modulo q and that is the product of exactly three primes, all of which are below $q^{\frac{3}{2}+\epsilon}$. If we restrict our attention to odd moduli q that do not have prime factors congruent to 1 mod 4, we can find such primes below $q^{\frac{11}{8}+\epsilon}$. If we further restrict our set of moduli to prime q that are such that $(q-1, 4\cdot 7\cdot 11\cdot 17\cdot 23\cdot 29) = 2$, we can find such primes below $q^{\frac{6}{5}+\epsilon}$. Finally, for any $\epsilon > 0$, there exists $q_0(\epsilon)$ such that when $q \geq q_0(\epsilon)$, there exists a natural number that is congruent to a modulo q and that is the product of exactly four primes, all of which are below $q(\log q)^6$.

Mathematics Subject Classification 2010: 11N13, 11A41, Secondary: 11N37, 11B13

Keywords: 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. The first author acknowledges the financial support by the Indian National Science Academy through a distinguished professorship. The second author was supported by the joint FWF-ANR project Arithrand: FWF: I 4945-N and ANR-20-CE91-0006.

1. Introduction and results

In this paper we investigate the representation of reduced residue classes modulo q by a product of exactly three small primes, and exceptionally by four of them in Theorem 1.4. We develop the approach initiated in [15], and followed up in [14], borrowing several results from the latter paper.

We input three new arguments: some vertical Brun-Titchmarsh inequalities (e.g. Theorems 5.1 and 6.1), the usage of P_2-numbers, see Theorem 3.2 and some additive combinatorics of sum-free sets in Section 4.

When using Kneser's theorem, we encounter two hurdles: the need to prove that the set of classes of small primes modulo q is dense enough, this is the job of the different versions of the Brun-Titchmarsh inequalities we employ, and the need to show that these primes do not stay in some union of cosets of some subgroup of small index in $(\mathbb{Z}/q\mathbb{Z})^\times$. By following the strategy of P.D.T.A. Elliott in [2], we prove that subgroups of index 5 contain small primes (we prove more, see Theorem 2.4). Finally Theorem 3.2 asserts that every coset of a small index subgroup contains either a small prime or a product of two of them. This is a consequence of the weighted sieve when using the approach we already put to work for the coset Brun-Titchmarsh inequality in [14]. The surprise is that, though we seem to be using the same kind of sieve argument as when bounding the density from above, the additive consequences are distinct. The additive combinatorial problem that emerges is investigated in Section 4. It relies on the combinatorics of sum-free sets.

Theorem 1.1. *Let $\epsilon > 0$. There exists q_0 such that for all $q \geq q_0$ and for all invertible residue classes a modulo q, there exists an integer congruent to a modulo q that is the product of exactly three primes, all of which are below $q^{\frac{3}{2}+\epsilon}$. When q is cube-free, we can find such primes below $q^{\frac{4}{3}+\epsilon}$.*

The main interest in the above result is that $\frac{3}{2} < 2$ while it is unknown whether there is such a small prime in any given arithmetic progression modulo q, the best bound for Linnik's constant under the Generalized Riemann Hypothesis being $2+\epsilon$.

We encounter two obstructions during the proof: the parity phenomenom and the large subgroups problem (arising from the usage of Kneser's theorem). We can avoid the second one by specializing the modulus q to a well-behaved family.

Theorem 1.2. *Let $\epsilon > 0$. There exists q_0 such that for every modulus $q \geq q_0$ all whose prime factors are congruent to 3 modulo 4, and for all invertible residue classes a modulo q, there exists an integer congruent to a modulo q that is the product of exactly three primes, all of which are below $q^{\frac{11}{8}+\epsilon}$.*

The same applies to integers q of the form $q = 4q'$ or $q = 8q'$ when all the prime factors of q' are congruent to 3 modulo 4. Notice for comparison that $11/8 = 1.375$.

Theorem 1.3. *Let $\epsilon > 0$. There exists p_0 such that for every prime $p \geq p_0$ such that $(p-1, 4\cdot 7\cdot 11\cdot 17\cdot 23\cdot 29) = 2$ and for all invertible residue classes a modulo p,*

there exists an integer congruent to a modulo p that is the product of exactly three primes, all of which are below $p^{\frac{6}{5}+\epsilon}$.

We can reach a smaller exponent for a general modulus by taking products of *four* primes, rather than of *three*.

Theorem 1.4. *There exist* q_0 *such that for all modulus* $q \geq q_0$ *and for all invertible residue classes a modulo q, there exists an integer congruent to a modulo p that is the product of exactly four primes, all of which are below* $q(\log q)^6$.

In [3], P. Erdős, A. Odlyzko and A. Sárközy proved that under the Generalized Riemann Hypothesis, we can find such a product of only two primes, and that under a weaker but still unproven hypothesis, we can find such a product of three primes. It is unclear to us how their method would work for products of four primes in case of the presence of a Siegel zero.

Thanks are due to the referee for his/her careful reading of this paper.

2. Primes in large subgroups modulo q

Lemma 2.1.

- *Given* $\epsilon > 0$, *there exists* $c(\epsilon) > 0$ *such that, for all real characters* χ *modulo q, we have* $|L(1,\chi)| > c(\epsilon)\, q^{-\epsilon}$.
- *There exists a constant* $c > 0$, *such that for all complex characters* χ *modulo q, we have* $|L(1,\chi)| \geq c/\log q$.

Lemma 2.2 (Burgess). *Let* χ *be a non-trivial character to modulus q. Then for all* X, $H \geq 1$, *and for all* $r \in \{1,2,3\}$, *we have the following: Given* $\epsilon > 0$, *there exists* $c(\epsilon)$, *such that*

$$\left| \sum_{X < n \leq X+H} \chi(n) \right| \leq c(\epsilon) H^{1-\frac{1}{r}} q^{\frac{r+1}{4r^2}+\epsilon}.$$

Further, if q is cube-free, one can take r to be any natural number.

The following is a consequence of the Burgess bounds.

Lemma 2.3. *For every character modulo q, we have*

- *If* $y \geq q^{1/3+\epsilon}$, *there is a* $\delta > 0$ *such that*

$$\sum_{n \leq y} \frac{\chi(n)}{n} = L(1,\chi) + O(q^{-\delta}).$$

The factor $1/3$ *can be replaced by* $1/4$ *when q is cube-free.*

- *Let $r \in \{1,2,3\}$ and suppose that $0 < \sigma < 1 - 1/r$. Then*

$$\sum_{n \le y} \frac{\chi(n)}{n^s} \ll \frac{y^{1-\sigma-\frac{1}{r}}}{1-\sigma-1/r}\, q^{\frac{r+1}{4r^2}+\epsilon}\,|s|.$$

Again, we can take any $r \ge 1$ when q is cubefree.

Theorem 2.4. *Let q be sufficiently large and $H \subseteq G_q = (\mathbb{Z}/q\mathbb{Z})^*$ be a subgroup of index Y. Then, there exists a prime $p \le c_0(\epsilon, Y) \cdot q_0^{\frac{Y-1}{3}+\epsilon}$, such that $p (mod\ q) \in H$. Further, if q is cube-free, one can replace the exponent $(Y-1)/3$ by $(Y-1)/4$.*

In [2], P.D.T.A. Elliott proved the same result when H is the set of invertible Y-th powers modulo prime q. Our proof follows along the similar lines. When $Y = 2$, the paper [17] of A.I. Vinogradov & Y. Linnik tells us that there is a prime $\ll q^{1/4+\varepsilon}$ in a quadratic subgroup modulo q *when q is prime*, a condition that has been removed by P. Pollack in [13]. In the case $Y \in \{3,4\}$ and q is prime, pertinent bounds may be found in [11] by T. Nagell and [1] by B. Kübra and P. Pollack.

Remark 2.1. To be more precise, the bound we obtain in Theorem 2.4 is of the form $c_1(\epsilon) \cdot \left(Y^3 q_0^{1/3+\epsilon}\right)^{Y-1}$.

To unfold the proof, we need to introduce the Dirichlet series given in (2.6), and this requires some preliminaries. The subgroup $\{\chi \in \hat{G}_q : \chi|_H = 1\}$ may be identified with characters on G_q/H. We further set $K = G_q/H$. Let $x > 1$ be such that none of the primes $p \le x$ falls into the subgroup H modulo q,

We define a multiplicative function $g(n)$as follows. Let

$$g(p) = \frac{1}{Y}\sum_{\chi \in \hat{K}} \chi(p) = \begin{cases} 1, & p \in H, \\ 0, & \text{otherwise}, \end{cases} \tag{2.1}$$

and $g(p^\alpha) = 0$ for all primes p and $\alpha \ge 2$. Our hypothesis on x implies that

$$g(p) = 0, \quad \text{for all primes } \ p \le x. \tag{2.2}$$

We let $g(1) = 1$. The Dirichlet series of $g(n)$ is given by

$$f(s) = \sum_{n=1}^{\infty} \frac{g(n)}{n^s} = \prod_p \left(1 + \frac{g(p)}{p^s}\right) = \prod_p \left(1 + \frac{1}{Y}\sum_{\chi \in \hat{K}} \frac{\chi(p)}{p^s}\right). \tag{2.3}$$

We find that

$$f(s)^Y = \omega(s) \prod_{\chi \in \hat{K}} L(s,\chi),$$

where $\omega(s)$ is Dirichlet series that is analytic for $\sigma > 1/2$. In fact

$$\omega(s) = \prod_p \left[\left(1 + \frac{g(p)}{p^s}\right)^Y \prod_{\chi \in \hat{K}} \left(1 - \frac{\chi(p)}{p^s}\right)\right]. \tag{2.4}$$

Let

$$\tilde{g} = \underbrace{g * \cdots * g}_{Y \text{ times}}, \quad \text{so that } f(s)^Y = \sum_n \frac{\tilde{g}(n)}{n^s}. \tag{2.5}$$

From (2.2), it follows that $\tilde{g}(p) = 0$ for all primes $p \le x$ and therefore $\tilde{g}(n) = 0$ for all $1 < n \le x$, except for $\tilde{g}(1) = 1$.

We now aim to obtain an asymptotic formula for the partial sums related to $\tilde{g}(n)$ using the Perron's formula. Since we are only interested in the sum of $\tilde{g}(n)$ with n not exceeding x, we find it convenient to consider the Dirichlet series obtained by truncating the L-functions at the parameter x (rather than considering $f(s)^Y$)

$$F(s) = \omega(s) L(s, \chi_{0,q})(s) \prod_{\substack{\chi \in \hat{K} \\ \chi \neq \chi_0}} \left(\sum_{n \le x} \frac{\chi(n)}{n^s} \right). \tag{2.6}$$

With this notation in hand, we may unfold our series of lemmas.

Lemma 2.5. *For $1/2 < \sigma \le 1$, we have $\zeta(2\sigma)^{-2Y} \le |\omega(s)| \le \zeta(2\sigma)^{2Y}$.*

Proof. We have

$$\begin{aligned} \log \omega(s) &= Y \sum_p \log\left(1 + \frac{g(p)}{p^s}\right) + \sum_{\chi \in \hat{K}} \sum_p \log\left(1 - \frac{\chi(p)}{p^s}\right) \\ &= Y \sum_{j=1}^{\infty} \frac{(-1)^{j-1}}{j} \sum_p \frac{g(p)^j}{p^{js}} - \sum_{j=1}^{\infty} \frac{1}{j} \sum_p \frac{1}{p^{js}} \sum_{\chi \in \hat{K}} \chi(p)^j. \end{aligned}$$

The contribution from $j = 1$ cancels out. Now, use the fact that $g(p)$ and $\chi(p)$ are bounded by 1, to obtain

$$\begin{aligned} |\log \omega(s)| &\le 2Y \sum_{j=2}^{\infty} \frac{1}{j} \sum_p \frac{1}{p^{j\sigma}} \le 2Y \sum_{j=1}^{\infty} \left(\frac{1}{2j} \sum_p \frac{1}{p^{2\sigma j}} + \frac{1}{2j+1} \sum_p \frac{1}{p^{\sigma(2j+1)}} \right) \\ &\le 2Y \log \zeta(2\sigma). \end{aligned}$$

□

Lemma 2.6. *Let $s = \sigma + it$. When $1/2 < \sigma = \Re s < 2/3$, we have*

$$F(s) \ll \left(\zeta^2(2\sigma) \frac{x^{2/3-\sigma}}{2/3 - \sigma} q_0^{1/9+\epsilon} \right)^{Y-1} (1 + |t|)^{Y - \frac{1}{2}}.$$

Proof. Using Lemma 2.3(b) with $r = 3$ and the bound

$$|L(s, \chi_{0,q})(s)| \ll q_0^{\epsilon} |t|^{\frac{1-\sigma}{2}} \ll q_0^{\epsilon} |t|^{1/2},$$

as well as the bound for $\omega(s)$ from Lemma 2.5, we find that

$$F(s) \ll \left(\zeta^2(2\sigma) \frac{x^{2/3-\sigma}}{2/3 - \sigma} q_0^{1/9+\epsilon} \right)^{Y-1} (1 + |t|)^{Y - \frac{1}{2}}.$$

The proof of the lemma is complete. □

Proof of Theorem 2.4. Let $\tilde{g} = \underbrace{g * \cdots * g}_{Y \text{ times}}$ be as in (2.5). We have seen that $\tilde{g}(1) = 1$ and $\tilde{g}(n) = 0$ for all $1 < n \le x$ owing to the hypothesis (2.2). Therefore

$$S = \frac{1}{\ell!} \sum_{n \le x} \tilde{g}(n) \left(\log \frac{x}{n}\right)^{\ell} = \frac{(\log x)^{\ell}}{\ell!}, \tag{2.7}$$

for any integer $\ell \ge 0$.

On the other hand, we use the following version of Perron's formula (assume $y \ne 1$ and $c > 1$):

$$\frac{1}{2\pi i} \int_{c-i\infty}^{c+i\infty} \frac{y^s}{s^{\ell+1}}\, ds = \begin{cases} \dfrac{(\log y)^{\ell}}{\ell!}, & y > 1, \\ 0, & \text{otherwise.} \end{cases}$$

As a result and with $\ell = Y + 1$, we find that

$$S = \frac{1}{2\pi i} \int_{2-i\infty}^{2+i\infty} F(s) \frac{x^s}{s^{\ell+1}}\, ds.$$

Moving the line of integration to $\Re(s) = \sigma$ $(1/2 < \sigma < 2/3)$ and collecting the residue at $s = 1$, we get

$$S = \mathrm{Res}_{s=1} F(s) \frac{x^s}{s^{\ell+1}} + \frac{1}{2i\pi} \int\limits_{\Re(s)=\sigma} F(s) \frac{x^s}{s^{\ell+1}}\, ds. \tag{2.8}$$

The main term above is controlled by Lemma 2.1:

$$\begin{aligned} \mathrm{Res}_{s=1} F(s) \frac{x^s}{s^{\ell+1}} &= x\omega(1) \frac{\varphi(q)}{q} \prod_{\substack{\chi \in \hat{K} \\ \chi \ne \chi_{0,q}}} \left(\sum_{n \le x} \frac{\chi(n)}{n} \right) \\ &\gg x \frac{\zeta(2)^{-2Y}}{\log\log q} \prod_{\substack{\chi \in \hat{K} \\ \chi \ne \chi_{0q}}} \big(L(1,\chi) + O(q^{-\delta})\big) \gg x q^{-\epsilon}, \end{aligned}$$

where we have used $\frac{\varphi(q)}{q} \gg \frac{1}{\log\log q}$ and the lower bound for $L(1,\chi)$ from Lemma 2.1. The implied constant depends on Y and ϵ. Choose

$$\sigma = 2/3 - \delta, \quad \text{with } \delta = \frac{1}{\log q}. \tag{2.9}$$

Using (2.6), the second term in (2.8) is at most

$$\begin{aligned} &\ll x^{2/3-\delta} \left(\zeta^2(4/3 - 2\delta)\, \delta^{-1} x^{\delta} q^{1/9+\epsilon} \right)^{Y-1} \int_1^{\infty} \frac{dt}{|t|^{3/2}} \\ &\ll x^{2/3+\delta(Y-2)} \left(13\, \delta^{-1} q^{1/9+\epsilon} \right)^{Y-1} \ll x^{2/3+\frac{Y}{\log q_0}} \left(13 q^{1/9+\epsilon} \log q \right)^{Y-1} \ll x q^{-2\epsilon}, \end{aligned}$$

as soon as $x \gg q^{\frac{Y-1}{3}+\epsilon}$. Hence

$$S \gg xq^{-\epsilon}.$$

On the other hand, we have from (2.7), that $S = \frac{(\log x)^\ell}{\ell!} = \frac{(\log x)^{Y+1}}{(Y+1)!} \ll x^\epsilon$, whenever $Y = o(\log x)$ (which is true since $\frac{Y}{\log x} \ll \frac{1}{\log q}$). This leads to a contradiction and completes the proof. □

3. Almost primes in cosets of large subgroups modulo q

Lemma 3.1 (Heath-Brown [8], Petrow & Young [12]). *Let χ be a Dirichlet character of conductor $r > 1$. When $1/2 \le \sigma = \Re s$, we have*

$$L(s,\chi) \ll_\varepsilon (r(|t|+1))^{\frac{3(1-\sigma)^+}{8}+\varepsilon}$$

valid for any $\varepsilon > 0$. Here $(1-\sigma)^+ = \max(0, 1-\sigma)$. When r is cube-free, one may replace $3/8$ by $1/3$.

Theorem 3.2. *There is a constant $C > 0$ such that, for every subgroup H of $(\mathbb{Z}/q\mathbb{Z})^\times$ of index Y and every coset $b \cdot H$, there exists a P_2-number that is of size not more than $C \cdot Y^{9/2} q^{0.768}$, where C is some effective constant. When q is cube-free, this size may be reduced to $C \cdot Y^{9/2} q^{0.683}$.*

By a "P_2-number", we mean an integer that has at most two prime factors. In [7], R. Heath-Brown proves that, for any a prime to q, there is a P_2-number of size $\ll q^{2-0.035}$ congruent to a modulo q, where the implied constant does not depend on a. We obtain an exponent < 1 for the cosets.

Proof. Let us use again the setting of the previous section. We start with a subgroup $H \subset G_q = (\mathbb{Z}/q\mathbb{Z})^\times$ of (small) index Y. Consider $\{\chi \in \hat{G}_q : \chi|_H = 1\}$. This can be identified with characters on $K = G_q/H$. Let $b \in G_q$. To find a small P_2-number in $b \cdot H$, we shall be using a special case of the main result of G. Greaves in [4] (or Chapter 5 of [5]) which we now state. Let $\mathcal{A} \subset [1, X^*]$ be a subset of integers. Assume that

$$\#\{a \in \mathcal{A}, d \text{ divides } a\} = \frac{X\rho(d)}{d} + R(\mathcal{A}, d) \quad \text{with } \rho(d) = \begin{cases} 1 & \text{when } (d,q) = 1, \\ 0 & \text{otherwise.} \end{cases} \tag{3.1}$$

Let y be a *level of distribution*, i.e. a real number such that

$$\sum_{d \le y} 3^{\omega(d)} |R(\mathcal{A}, d)| \ll \frac{X}{\log^2 X}. \tag{3.2}$$

Then, if $X^* \le y^g$ where $g = 2 - 0.004456$, then there exists $a \in \mathcal{A}$ having at most two prime factors.

Define $X^* = \frac{q}{\varphi(q)} YX$ and

$$\mathcal{A} = \big\{a : a \le X^*, a \text{ falls inside } b \cdot H\big\}. \tag{3.3}$$

Let us verify the conditions of the result of Greaves.

We decompose the characteristic function of $b \cdot H$ through multiplicative characters, i.e. we write

$$1_{b\cdot H} = \frac{1}{Y} \sum_{\chi \in \hat{K}} \overline{\chi}(b)\chi.$$

On defining $A_d(s) = \sum_{d|n\geq 1} 1_{\mathcal{A}}(n)/n^s$, the truncated Perron summation formula gives us

$$\sum_{\substack{n\in\mathcal{A},\\ d|n}} 1 = \frac{1}{2i\pi} \int_{\kappa-iT}^{\kappa+iT} A_d(s) \frac{X^{*s} ds}{s} + O\Big(\frac{X^* \log^2 X^*}{dT} \Big)$$

provided that $1 \leq T^2 \leq X^*/d$ and where $\kappa = 1 + 1/(\log X^*)$. This expands into

$$\sum_{\substack{n\in\mathcal{A},\\ d|n}} 1 = \frac{1}{Y} \sum_{\chi \in \hat{K}} \overline{\chi}(b)\chi(d) \frac{1}{2i\pi} \int_{\kappa-iT}^{\kappa+iT} L(s,\chi) \frac{X^{*s} ds}{d^s s} + O\Big(\frac{X^* \log^2 X^*}{dT} \Big).$$

We recall Lemma 3.1, and deduce that

$$\sum_{\substack{n\in\mathcal{A},\\ d|n}} 1 - \frac{1}{Y} \frac{\varphi(q)}{q} \frac{X^*}{d} 1_{(d,q)=1} \ll \frac{X^* \log^2 X^*}{dT} + \frac{(qT)^{3/16+\varepsilon}\sqrt{X^*}}{\sqrt{d}}.$$

With $R(\mathcal{A}, d)$ defined in (3.1), we deduce from the above that

$$\sum_{d\leq y} 3^{\omega(d)} |R(\mathcal{A}, d)| \ll \sqrt{yX^*}(Tq)^{3/16+\varepsilon} + \frac{X^* \log^9(yX^*)}{T} \tag{3.4}$$

for any positive ε. In particular we can choose $\delta > 0$ and take $T = Y(\log q)(\log X^*)^{11}$ together with $y = X/(Y^{1+3/8} q^{\delta+3/8}) \geq 1$ and obtain

$$\sum_{d\leq y} 3^{\omega(d)} |R(\mathcal{A}, d)| \ll_\delta X/(\log X)^2. \tag{3.5}$$

As a conclusion, we can find a P_2 in $\mathcal{A}$ provided that

$$g = \frac{\log X^*}{\log y} \leq 2 - 0.044560 \tag{3.6}$$

i.e.

$$X \geq Y^{\frac{11}{8}\frac{3-0.044560}{1-0.044560}} q^{(\frac{3}{8}+\delta)\frac{2-0.044560}{1-0.044560}}. \tag{3.7}$$

We find that $\frac{3}{8} \times \frac{2-0.044560}{1-0.044560} = 0.7674\cdots \leq 4/5$ and $\frac{11}{8} \times \frac{3-0.044560}{1-0.044560} = 4.2532\cdots \leq 9/2$. When q is cube-free, we use the refined bound also recalled in Lemma 3.1. □

4. Some additive combinatorics

Our final results involves usage of additive combinatorics, but the additive combinatorics problem we address can be formulated independently. We do so, as it leads to a better understanding of what we do/don't know how to prove.

We thus start with a finite abelian group G written additively. We also recall for completeness that, when $\mathcal{A}$ and $\mathcal{B}$ are two subsets of some abelian group G, the sum $\mathcal{A}+\mathcal{B}$ is defined by

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

In particular, the number of representations of a given element is not taken into account. We use the shortcuts $2\mathcal{A}=\mathcal{A}+\mathcal{A}$ and $3\mathcal{A}=\mathcal{A}+\mathcal{A}+\mathcal{A}$. The stabilizer, say H, of a subset $\mathcal{C}$ of G is the subgroup defined by

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

Lemma 4.1. *A subset $\mathcal{C}$ of a finite abelian group is a union of cosets modulo its stabilizer.*

Proof. On denoting by H this stabilizer, it is enough to check that, given any element c from $\mathcal{C}$, we indeed have $c+H\subset\mathcal{C}$. This follows from the definition of the stabilizer. In group theoretical parlance, $\mathcal{C}$ is *saturated* modulo H. The lemma follows swiftly. □

Lemma 4.2. *Let $\mathcal{A}$ be a subset of a finite abelian group and let H be the stabilizer of $\mathcal{A}+\mathcal{A}$. Then $\mathcal{A}+\mathcal{A}+\mathcal{A}$ is also a union of cosets modulo H.*

Proof. This follows from the equation $\mathcal{A}+\mathcal{A}+\mathcal{A}=\mathcal{A}+2\mathcal{A}=\mathcal{A}+(2\mathcal{A}+H)$. □

4.1. *Auxiliary lemmas*

Lemma 4.3. *Let $\mathcal{A}$ be a subset of a finite abelian group G. Let H be the stabilizer of $\mathcal{A}+\mathcal{A}$. Suppose that $\mathcal{A}$ meets λ cosets of H. Then*

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

This is [14, Corollary A.2], a corollary of the famous Kneser's Theorem. While Lemma 4.3 is used when the sets we add have a somewhat small cardinality, the next lemma is tailored for very large sets.

Lemma 4.4. *Let $\mathcal{A}$ and $\mathcal{B}$ be two subsets of a finite abelian group G satisfying $|\mathcal{A}|+|\mathcal{B}|>|G|$. Then $\mathcal{A}+\mathcal{B}=G$.*

This is [14, Lemma 5.1].

Lemma 4.5. *Let $\mathcal{A}$ be a subset of a finite abelian group G such that $|\mathcal{A}| \geq \eta|G|$, with $\eta > 1/3$. Define, for any integer Y,*

$$\lambda(Y) = \begin{cases} \lceil \eta Y \rceil + 1 & \text{when } Y \equiv 2[3] \text{ and } 2 \leq Y \leq 1/(3\eta - 1), \\ \lceil \eta Y \rceil & \text{otherwise.} \end{cases}$$

For any subgroup H of index Y, assume $\mathcal{A}$ meets at least $\lambda(Y)$ cosets. Then $\mathcal{A} + \mathcal{A} + \mathcal{A} = G$.

As $|\mathcal{A}|/|H| \geq \eta Y$, the subset $\mathcal{A}$ always meets at least $\lceil \eta Y \rceil$ cosets modulo H.

Proof. Let H be the stabilizer of $2\mathcal{A}$. By Lemmas 4.3 and 4.4, we have $3\mathcal{A} = G$ as soon as $|\mathcal{A}| + |\mathcal{A} + \mathcal{A}| > |G|$, hence as soon as

$$|\mathcal{A}| + (2\lambda - 1)|H| > |G|.$$

Since $|\mathcal{A}|/H \geq \eta Y$, this is certainly true if $\eta Y + 2\lambda - 1 > Y$, and, since $\lambda \geq \eta Y$, this holds when $Y > 1/(3\eta - 1)$. This explains the change of definition of $\lambda(Y)$ according to whether Y is smaller or larger than $1/(3\eta - 1)$. When Y is larger, we only use the rather trivial value $\lambda(Y) = \lceil \eta Y \rceil$.

Let us now turn to the non-trivial case $Y \leq 1/(3\eta - 1)$. By Lemma 4.1, the set $2\mathcal{A}$ is a union of cosets modulo H, and by Lemma 4.3, of at least $2\lambda - 1$ of them. This implies that $\mathcal{A} + \mathcal{A} + \mathcal{A}$ contains at least $3\lambda - 2$ cosets modulo H. Let us write $Y = 3y + a$ for $a \in \{0, 1, 2\}$. We have $\lceil \eta Y \rceil > y + \frac{a}{3}$, and thus $\lceil \eta Y \rceil \geq y + 1 = \frac{Y}{3} + \frac{3-a}{3}$. This implies that $3\lambda - 2 \geq Y + 1 - a$. When $a \in \{0, 1\}$, this is at least Y, meaning that $\mathcal{A} + \mathcal{A} + \mathcal{A} = G$. When $Y \equiv 2[3]$, i.e. when $a = 2$, and $Y \leq 1/(3\eta - 1)$, our hypothesis gives us the better bound $\lambda \geq \lceil \eta Y \rceil + 1$. This is enough to complete the proof. □

4.2. *Setting the problem and preliminary conclusions*

Let $\mathcal{A}$ be a subset of G such that

$$|\mathcal{A}| \geq \eta|G|, \quad \eta > 1/3. \tag{4.1}$$

Our problem is to find hypotheses that will lead to the conclusion that $3\mathcal{A} = G$.

Having Lemma 4.3 in mind, we consider the stabilizer H of $2\mathcal{A} = \mathcal{A} + \mathcal{A}$. Here are some facts and further definitions:

(1) $2\mathcal{A}$ and $3\mathcal{A}$ are both a union of H-cosets, by Lemma 4.1 and 4.2.
(2) On setting $G^* = G/H$ and $\mathcal{A}^* = \mathcal{A}/H$, it is enough to show that $3\mathcal{A}^* = G^*$. This is true even if H does not stabilize $\mathcal{A}$, since we readily check that $3\mathcal{A} = 3\mathcal{A} + H = 3(\mathcal{A} + H)$.
(3) Notice that $2\mathcal{A}^*$ has a trivial stabilizer in G^*.
(4) We set $Y = |G/H| = |G^*|$ and $\lambda = |\mathcal{A}/H|$ so that $|2\mathcal{A}^*| \geq 2\lambda - 1$ by Lemma 4.3.

As a conclusion of Lemma 4.5 and given η, only a finite number of values of Y, the index of H, are to be considered, and they are all congruent to 2 modulo 3. Once

these general considerations are set, let us turn to the hypotheses we are ready to assume. Here are the first two:

[C_0] The subset $\mathcal{A}$ generates G. This is an obvious hypothesis which is in fact implied by our other assumptions.

[C_1] The subset $\mathcal{A}$ has a non-empty intersection with every coset of any subgroup of index 2.

Here are two additional series of hypotheses we are considering:

[$C_2(Y_0)$] The subset $\mathcal{A}$ intersects every subgroup of index at most Y_0 and congruent to 2 mod 3.

[$C_3(Y_0)$] Let K be a subgroup of G of index at most Y_0 and congruent to 2 mod 3. The subset $\mathcal{A} \bigcup 2\mathcal{A}$ has a non-empty intersection with every coset modulo K.

Please notice that hypothesis [$C_2(Y_0)$] does not ask anything concerning the coset $u + K$ when $u \notin K$, while hypothesis [$C_3(Y_0)$] ensures that an element of $\mathcal{A}$ *or* of $2\mathcal{A}$ belongs to it.

Lemma 4.6. *Let $\mathcal{A}^*$ be a subset of a finite abelian group G^* satisfying $\mathcal{A}^* \cup 2\mathcal{A}^* = G^*$ and such that the stabilizer of $2\mathcal{A}^*$ is $\{0\}$. Then either $3\mathcal{A}^* = G^*$ or we have the five conditions*

- $0 \notin \mathcal{A}^*$ *and* $\mathcal{A}^* = -\mathcal{A}^*$,
- *The stabilizer of* $\mathcal{A}^*$ *is* $\{0\}$,
- $\mathcal{A}^* \cap 2\mathcal{A}^* = \emptyset$,
- $|\mathcal{A}^*| \le (|G^*| + 1)/3$,
- $3\mathcal{A}^* = G^* \setminus \{0\}$.

In any case, when $|G^*| > 2$, we have $4\mathcal{A}^* = G^*$.

Note that the third condition tells us that $\mathcal{A}^*$ is a sum-free set of the finite abelian group G^*. Moreover, the fifth one is a consequence of the first four. Such sets have been studied, for instance in [18] and in [6]. We ran some numerical experiments when G^* is the cyclic group with ℓ elements say to detect the existence of the second case of the above lemma. We found that the situation is quite rigid but not completely so. Here are some examples:

- $\mathcal{A}^* = \{2, 3\}$ mod 5 is our basic example.
- We explored $\ell \le 29$ with Sage [16] and here are the size of the sets $\mathcal{A}^*$ that are possible:

ℓ	8	11	17	18	19	20	21	22	23	24	25	26	27	28	29
$\lvert\mathcal{A}^*\rvert$	3	4	6	6	6	6,7	6	7	8	7,8	8	7,8,9	8	8,9	8,10

- A small cardinality example modulo 71 is given by $\mathcal{C} \cup (-\mathcal{C})$ where $\mathcal{C} = \{1, 3, 5, 17, 26, 30, 32\}$ mod 71.

Proof. If $0 \in \mathcal{A}^*$, the assumption $\mathcal{A}^* \cup 2\mathcal{A}^* = G^*$ readily implies that $3\mathcal{A}^* = G^*$. Let us consider

$$\Gamma = \left\{ g / (g - \mathcal{A}^*) \cap 2\mathcal{A}^* = \emptyset \right\} = G^* \setminus 3\mathcal{A}^*$$

which we assume to be non-empty. Let $g \in \Gamma$. Since $g - \mathcal{A}^*$ has no intersection with $2\mathcal{A}^*$, it has to be included within $\mathcal{A}^*$. But since the cardinalities of $\mathcal{A}^*$ and of $g - \mathcal{A}^*$ are the same, we have $g - \mathcal{A}^* = \mathcal{A}^*$. Let g_1 and g_2 be two elements of Γ. We have $g_1 - (g_2 - \mathcal{A}^*) = (g_1 - g_2) + \mathcal{A}^*$ on the one hand, while $g_1 - (g_2 - \mathcal{A}^*) = g_1 - \mathcal{A}^* = \mathcal{A}^*$ on the other one. This means that $g_1 - g_2$ stabilizes $\mathcal{A}^*$, hence it stabilizes $2\mathcal{A}^*$, which means that it vanishes. We have thus proved that Γ is reduced to a single point, say g_0. We have $\mathcal{A}^* \cap 2\mathcal{A}^* = g_0 - \mathcal{A}^* \cap 2\mathcal{A}^* = \emptyset$.

We also find that $g_0 - 2\mathcal{A}^* = 2\mathcal{A}^*$ and that $2\mathcal{A}^* = (g_0 - \mathcal{A}^*) + (g_0 - \mathcal{A}^*) = 2g_0 - 2\mathcal{A}^*$. This implies that $2\mathcal{A}^* = g_0 + (g_0 - 2\mathcal{A}^*) = g_0 + 2\mathcal{A}^*$, i.e. that g_0 stabilizes $2\mathcal{A}^*$. It is thus equal to 0, i.e. $3\mathcal{A}^* = G^* \setminus \{0\}$. Furthermore, Kneser's Theorem (Lemma 4.3 is enough) tells us that $|2\mathcal{A}^*| \geq 2|\mathcal{A}^*| - 1$, and since $|\mathcal{A}^*| + |2\mathcal{A}^*| = |G^*|$, we get $|\mathcal{A}^*| \leq (|G^*| + 1)/3$. This upper bound also implies that $2|2\mathcal{A}^*| \geq 2(2|G^*| - 1)/3 > |G^*|$ when $|G^*| > 2$. □

4.3. *Results*

Theorem 4.7. *Let $\mathcal{A} \subset G$ be a subset of the finite abelian group G that is such that $|\mathcal{A}|/|G| > 2/5$. On assuming $[C_0]$ and $[C_1]$, we have $3\mathcal{A} = G$.*

The previous two papers [15] and [14] relied on this result.

Proof. Let us set $\eta = |\mathcal{A}|/|G|$. As $1/(3\eta - 1)$ is less than 5, Lemma 4.5 tells us that only subgroups of index 2 may give rise to a difficulty, but this is avoided by $[C_0]$ and $[C_1]$. □

Theorem 4.8. *Let $\mathcal{A} \subset G$ be a subset of the finite abelian group G that is such that $|\mathcal{A}|/|G| > 3/8$. On assuming $[C_0]$, $[C_1]$, $[C_2(5)]$ and $[C_3(5)]$, we have $3\mathcal{A} = G$.*

This is the main novelty of the present paper on the additive combinatorics side.

Proof. Let us set $\eta = |\mathcal{A}|/|G|$. As $1/(3\eta - 1)$ is less than 8, Lemma 4.5 tells us that only subgroups of index 2 or 5 may give a difficulty. The case $Y = 2$ is ruled out by $[C_0]$ and $[C_1]$. In case $Y = 5$, by $[C_3(5)]$, Lemma 4.6 applies. It tells us that $H \bigcap \mathcal{A} = \emptyset$, which is assumed to be false by $[C_2(5)]$. □

Theorem 4.9. *Let $\mathcal{A} \subset G$ be a subset of the finite abelian group G that is such that $|\mathcal{A}|/|G| = \eta > 1/3$. Set $Y_0 = 1/(3\eta - 1)$. On assuming $[C_0]$, $[C_1]$, $[C_2(Y_0)]$ and $[C_3(Y_0)]$, we have $3\mathcal{A} = G$.*

Remark 4.1. This theorem shows that in our setting when $G = (\mathbb{Z}/q\mathbb{Z})^\times$ and $\mathcal{A} = \{p \leq q^{1+\varepsilon}, (p, q) = 1\}$, the Lindelöf hypothesis in q-aspect for the Dirichlet L-functions is enough to obtain the conclusion, as we prove Assumption $[C_3(Y_0)]$ in Theorem 3.2, when q is large enough, and the proof of Theorem 2.4 easily gets adapted to show that $[C_2(Y_0)]$ also holds, again when q is large enough.

Proof. The proof of Theorem 4.8 is immediately adapted to this case. □

The above results can be sharpened when looking more closely at the structure of small examples. Here is such a sharpening.

Theorem 4.10. *Let $\mathcal{A} \subset G$ be a subset of the finite abelian group G that is such that $|\mathcal{A}|/|G| = \eta > 4/11$. On assuming $[C_0]$, $[C_1]$, $[C_2(5)]$, $[C_3(8)]$ and that the 2-part of G is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^r$ for some $r \geq 0$, we have $3\mathcal{A} = G$.*

Proof. We adapt the proof of Theorem 4.9 and readily discover that we only have to worry about the case $Y = 8$. Our assumption imples that $G^* = G/H$ is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^3$. By Lemma 4.6, we may have difficulties when $\mathcal{A}^* = \mathcal{A}/H$ has cardinality 3. But since $\mathcal{A}^*$ generates G^* that may be viewed as a vector space of dimension 3, $\mathcal{A}^*$ is thus a basis of G^*, which would contradict the fact that $\mathcal{A}^* \bigcup 2\mathcal{A}^* = G^*$. □

5. Three primes. Proof of Theorems 1.1, 1.2 and 1.3

By using the techniques of Iwaniec in [9, Section 2] (as noted by H. Mikawa in [10]), one can prove the next lemma.

Lemma 5.1 (Iwaniec [9]). *Let $\varepsilon \in (0, 1/200)$ and $\epsilon' > 0$ be given. For almost all a modulo $q \geq q_0(\varepsilon, \epsilon')$ and $q^{\frac{6}{5}+\varepsilon} \leq X$, we have*

$$\pi(x; q, a) \leq \frac{2(1+\epsilon')X/\varphi(q)}{\log(X/q^{3/8})}.$$

Proof of Theorem 1.1. Let $\mathcal{P}(y)$ be the set of primes below y that do not divide q and let $\mathcal{A}$ be the image of $\mathcal{P}(y)$ in $G_q = (\mathbb{Z}/q\mathbb{Z})^\times$. We seek to show that $\mathcal{A}\cdot\mathcal{A}\cdot\mathcal{A} = G_q$. We select $X = q^{3/2+\epsilon}$. We compute that

$$\frac{\log(X/q^{3/8})}{2\log X} = \frac{3}{8} + \frac{\epsilon}{12+8\epsilon}. \tag{5.1}$$

We use Lemma 5.1. Outside of a set of density ϵ'', we have the stated inequality from which we infer find that

$$\frac{|\mathcal{A}|}{\varphi(q)} \geq \frac{3}{8(1+\epsilon')} + \frac{\epsilon/(1+\epsilon')}{12+8\epsilon} - \epsilon'' > 3/8 \tag{5.2}$$

on selecting ϵ' and ϵ'' properly. To be precise, on assuming $\epsilon \leq 1$ and $\epsilon' \leq 1/2$, we find that

$$\begin{aligned}\frac{3}{8(1+\epsilon')} + \frac{\epsilon/(1+\epsilon')}{12+8\epsilon} - \epsilon'' &\geq \frac{3}{8} - \frac{3\epsilon'}{8} + \frac{\epsilon(1-\epsilon')}{20} - \epsilon'' \\ &\geq \frac{3}{8} - \frac{3\epsilon'}{8} + \frac{\epsilon}{40} - \epsilon''.\end{aligned}$$

We select $\epsilon' = \epsilon'' = \epsilon/100$. Theorem 4.9 applies, the hypotheses being met by Theorem 2.4 with $Y = 2$, then with $Y = 5$, and by Theorem 3.2 for index $Y = 5$.□

Proof of Theorem 1.2. Again, let $\mathcal{P}(y)$ be the set of primes below y that do not divide q and let $\mathcal{A}$ be the image of $\mathcal{P}(y)$ in $G_q = (\mathbb{Z}/q\mathbb{Z})^\times$. We seek to show that $\mathcal{A}\cdot\mathcal{A}\cdot\mathcal{A} = G_q$. We select $X = q^{11/8+\epsilon}$. We compute that

$$\frac{\log(X/q^{3/8})}{2\log X} = \frac{4}{11} + \frac{12\epsilon}{121+88\epsilon}. \tag{5.3}$$

We proceed as for the proof of Theorem 1.1 with Lemma 5.1. We find that

$$\frac{|\mathcal{A}|}{\varphi(q)} > 4/11. \tag{5.4}$$

Theorem 4.8 applies, the hypotheses again being met by Theorem 2.4 with $Y = 2$, then with $Y = 5$ and by Theorem 3.2 for index $Y = 5$. The special hypothesis concerning the 2-part of $\mathcal{A}$ is ensured by the our assumption on q. □

Proof of Theorem 1.3. We take $X \geq p^{\frac{6}{5}+\epsilon}$ and p large enough in terms of ϵ. We find that

$$\eta = |\mathcal{A}|/\varphi(p) > \frac{11}{32}.$$

Since $1/(3 \times \frac{11}{32} - 1) = 32$, the only Y giving trouble are congruent to 2 modulo 3 and ≤ 32. Theorem 4.9 asks for $[C_3(32)]$, which is granted by Theorem 3.2, and for $[C_2(32)]$. We check numerically that this may happen only when $Y \in \{8, 11, 14, 17, 20, 23, 26, 29, 32\}$. Our hypothesis on p excludes all these cases, as Y has to be a divisor of $\varphi(p) = p - 1$. □

6. Four primes. Proof of Theorem 1.4

Mikawa in [10] proved the next result (be careful: on page 31, the theorem is stated with a power $(\log x)^{-A}$ but the $-$ sign faded. The correct result is on page 33, line -3).

Lemma 6.1 (Mikawa [10]). *Let $\epsilon' > 0$ and $A > 5$ be given. For almost all a modulo $q \geq q_0(\epsilon', A)$, we have*

$$\pi(x; q, a) \leq \frac{(2+\epsilon')x/\varphi(q)}{\log(x^{2/3}/q^{1/9})}, \quad x^{6/7} \leq q \leq x/(\log x)^A.$$

Proof of Theorem 1.4. As in the proof of Theorem 1.1, let $\mathcal{P}(y)$ be the set of primes below y that do not divide q and let $\mathcal{A}$ be the image of $\mathcal{P}(y)$ in $G_q = (\mathbb{Z}/q\mathbb{Z})^\times$. We seek to show that $\mathcal{A}\cdot\mathcal{A}\cdot\mathcal{A}\cdot\mathcal{A} = G_q$. We set $X = q(\log q)^6$. Hence $q \leq X/(\log X)^5$ if q is large enough. By Lemma 6.1, we have

$$|\mathcal{A}|/\varphi(q) \geq \frac{\log(x^{2/3}/q^{1/9})}{(2+\epsilon')\log x} - \varepsilon \geq \frac{5\log(X\log X)}{9(2+\epsilon')\log X} - \varepsilon \geq \frac{5}{18} - O(\varepsilon) \geq 0.2777$$

since $5/18 = 0.2777\ldots$ and by selecting ϵ sufficiently small. Let H be the stabilizer of $\mathcal{A}\cdot\mathcal{A}$, with index Y and define $|\mathcal{A}/H| = n \geq \lceil 0.2777 \cdot Y \rceil$. By using Lemma 4.3,

we get

$$\frac{2|\mathcal{A}\cdot\mathcal{A}|}{\varphi(q)} \geq 2\frac{2\lceil 0.2777\cdot Y\rceil - 1}{Y}.$$

The inequality $\lceil 0.2777\cdot Y\rceil \geq 0.2777Y$ shows that this quantity is > 1 when $Y \geq 55$. When Y is smaller, we first notice that $Y = 2$ is ruled out by Theorem 2.4. Next, we may apply Theorem 3.2. On the one hand, by Lemma 4.3, we have $|2\mathcal{A}/H| \geq 2n-1$, while, by Theorem 3.2, we also have $|\mathcal{A}/H|+|2\mathcal{A}/H| \geq Y$. This implies that $|2\mathcal{A}/H|$ is at least $Y-n$. Thus $|2\mathcal{A}/H|$ is at least $\max(2n-1, Y-n)$ which is greater than $(2Y-1)/3$. As $2(2Y-1)/3 > Y$ when $Y \geq 3$, we conclude that $3\mathcal{A} = G_q$, as required. □

References

[1] Kübra Benli and P. Pollack. Small prime kth power residues for $k = 2, 3, 4$: a reciprocity laws approach. *Proc. Amer. Math. Soc.*, 147(3):987–994, 2019.

[2] P. D. T. A. Elliott. The least prime $k-$ th-power residue. *J. London Math. Soc. (2)*, 3:205–210, 1971.

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

[4] G. Greaves. The weighted linear sieve and Selberg's λ^2-method. *Acta Arith.*, 47(1):71–96, 1986.

[5] G. Greaves. *Sieves in number theory*, volume 43 of *Ergebnisse der Mathematik und ihrer Grenzgebiete*. Springer-Verlag, Berlin, 2001. xii+304 pp.

[6] Ben Green and Imre Z. Ruzsa. Sum-free sets in abelian groups. *Israel J. Math.*, 147:157–188, 2005.

[7] D. R. Heath-Brown. Almost-primes in arithmetic progressions and short intervals. *Math. Proc. Cambridge Philos. Soc.*, 83(3):357–375, 1978.

[8] D. R. Heath-Brown. Hybrid bounds for Dirichlet L-functions. II. *Quart. J. Math. Oxford Ser. (2)*, 31(122):157–167, 1980.

[9] Henryk Iwaniec. On the Brun-Titchmarsh Theorem. *J. Math. Soc. Japan*, 34(1):95–123, 1982.

[10] Hiroshi Mikawa. On the Brun-Titchmarsh Theorem. *Tsukuba J. Math.*, 15(1):31–40, 1991.

[11] Trygve Nagell. Sur les restes et les non-restes cubiques. *Ark. Mat.*, 1:579–586, 1952.

[12] Ian Petrow and Matthew P. Young. The weyl bound for dirichlet l-functions of cube-free conductor. *Annals of Math.*, 2020.

[13] P. Pollack. The smallest prime that splits completely in an abelian number field. *Proc. Amer. Math. Soc.*, 142(6):1925–1934, 2014.

[14] O. Ramaré and Priyamvad Srivastav. Products of primes in arithmetic progressions. *Int. Journal of Number Theory*, 16(4):747–766, 2020. Appendix by O. Serra.

[15] O. Ramaré and Aled Walker. Products of primes in arithmetic progressions: a footnote in parity breaking. *J. Number Theory of Bordeaux*, 30(1):219–225, 2018.

[16] W. A. Stein et al. *Sage Mathematics Software (Version 5.9)*. The Sage Development Team, 2013. `http://www.sagemath.org`.

[17] A. I. Vinogradov and Ju. V. Linnik. Hypoelliptic curves and the least prime quadratic residue. *Dokl. Akad. Nauk SSSR*, 168:259–261, 1966.

[18] H. P. Yap. Maximal sum-free sets in finite abelian groups. V. *Bull. Austral. Math. Soc.*, 13(3):337–342, 1975.