PRODUCTS OF SMALL INTEGERS IN RESIDUE CLASSES AND ADDITIVE PROPERTIES OF FERMAT QUOTIENTS

GLYN HARMAN AND IGOR E. SHPARLINSKI

ABSTRACT. We show that for any $\varepsilon > 0$ and a sufficiently large cube-free q, any reduced residue class modulo q can be represented as a product of 14 integers from the interval $[1, q^{1/4e^{1/2}+\varepsilon}]$. The length of the interval is at the lower limit of what is possible before the Burgess bound on the smallest quadratic nonresidue is improved. We also consider several variations of this result and give applications to Fermat quotients.

1. INTRODUCTION

As usual, we say that an integer n is y-smooth if all prime divisors $p \mid n$ satisfy $p \leq y$. We write

$$\beta = \frac{1}{4} e^{-1/2}.$$

By a result of Harman [19, Theorem 3] for any $\varepsilon > 0$ and a sufficiently large cube-free q, every reduced residue class modulo q contains a $q^{\beta+\varepsilon}$-smooth positive integer $s \leq q^{9/4+\varepsilon}$. Clearly this result is the best possible (in terms of β) until at least the Burgess bound [4, 5] on the smallest quadratic nonresidue is improved. Harman [19, Theorem 3] also gives similar, albeit weaker, results for non cube-free moduli q.

Here we are mostly interested in the number of small factors of n rather than in its size. More precisely our goal is to minimize the values of k such that for any $\varepsilon > 0$ and a sufficiently large cube-free q, for any integer a with $\gcd(a, q) = 1$, there is always a solution to the congruence

$$(1) \qquad n_1 \ldots n_k \equiv a \pmod{q}, \qquad 1 \leq n_1, \ldots, n_k \leq q^{\beta+\varepsilon}.$$

We remark that $\beta = 0.1516\ldots$ and it is certainly the limit of what one may hope to obtain without improving the Burgess bound [4] on the smallest quadratic non-residue. For large intervals, several results in this direction have been obtained by Garaev [14]. For example,

Garaev [14] notices that for any $\varepsilon > 0$ and a sufficiently large cube-free q every a with $\gcd(a, q) = 1$ can be represented modulo q as a product of $k = 8$ positive integers up to $q^{1/4+\varepsilon}$ (which is an immediate consequence of [14, Theorem 2]). It is a feature of all current methods that if our variables are of size q^{ϑ} then we require $k\vartheta > 2$. In that sense both our result with $k = 14$ and that of Garaev [14] are best possible at present (note that $13\beta < 2$). Several related questions, also involving multiplicative subgroups of the unit group $\mathbb{Z}_q^*$ of the residue ring modulo q, have been studied by Cilleruelo and Garaev [9].

Note that although formally [19, Theorem 3] does not give any upper bound on the number of factors in a $q^{\beta+\varepsilon}$-smooth positive integer $s \leq q^{9/4+\varepsilon}$ with $s \equiv a \pmod{q}$ such a bound can easily be derived via simple combinatorial arguments. More precisely, one combines together prime divisors of n in a greedy way into factors of size at most $q^{\beta+\varepsilon}$. The argument of [19] is flexible enough to impose additional restrictions on the prime factors of the integers s to solve (1) with $k = 18$ and with more work that can be reduced to $k = 16$. We can do a little better, however, by combining this approach with the ideas of Balog [1] and Garaev [14] to derive the following result.

Theorem 1. *For any $\varepsilon > 0$ and a sufficiently large cube-free q, for any integer a with $\gcd(a, q) = 1$, there is always a solution to the congruence (1) with $k = 14$.*

Some of our motivation to investigate the solvability of (1) for small values of k comes from studying the additive properties of the *Fermat quotient* $q_p(u)$ modulo a prime p, which is defined as the unique integer with

$$q_p(u) \equiv \frac{u^{p-1} - 1}{p} \pmod{p}, \qquad 0 \leq q_p(u) \leq p - 1.$$

We also define

$$q_p(kp) = 0, \qquad k \in \mathbb{Z}.$$

Clearly the function $q_p(u)$ is periodic with period p^2. For any integers r, u and v with $\gcd(uv, p) = 1$ we have

$$(2) \qquad\qquad q_p(u) + q_p(v) \equiv q_p(uv) \pmod{p}$$

and

$$(3) \qquad\qquad q_p(u + rp) \equiv q_p(u) - ru^{-1} \pmod{p},$$

see, for example, [11, Equations (2) and (3)].

Fermat quotients appear in various questions of computational and algebraic number theory, see the survey [11] of classical results and also [2, 21, 27, 32] for results about vanishing Fermat quotients, [7, 8,

20, 26, 30, 31] for results about the distribution, fixed points and value set and [6, 15, 28, 29, 30] for bounds of exponential and multiplicative character sums.

Furthermore, Chen and Winterhof [8] have recently studied additive properties of Fermat quotients and their generalisations. In particular, Chen and Winterhof [8] study the question of solvability of the congruence

$$(4) \qquad q_p(u_1) + \ldots + q_p(u_k) \equiv a \pmod{p}, \qquad 1 \le u_1, \ldots, u_k \le U,$$

for some fixed integer k and a sufficiently large parameter U (and also a congruence with a generalisation of Fermat quotients). Clearly the method of [8], based on bounds of exponential sums has a natural limit of $U \ge p^{1/2+\varepsilon}$ for an arbitrary small $\varepsilon > 0$ coming from the non-triviallity range of the Burgess bound, see [4, 5] and also [22, Theorem 12.6] for a modern treatment. Here, we observe that Theorem 1 applied with $q = p^2$ and combined with (2) and (3) allows us to study (4) for much smaller values of U. Indeed, it follows from (3) that for any integer b with $\gcd(b, p) = 1$, there exists an integer a with $\gcd(a, p) = 1$ such that $q_p(a) \equiv b \pmod{p}$. Hence, we derive from Theorem 1 that for any $\varepsilon > 0$, a sufficiently large prime p and $U \ge p^{1/2e^{1/2}+\varepsilon}$, for any integer a with $\gcd(a, p) = 1$, there is always a solution to the congruence (4) with $k = 14$.

In actual fact it is more efficient to analyse the problem of Fermat quotients more closely and establish a variant of Theorem 1 for the congruence

$$(5) \qquad n_1 \ldots n_k \equiv au \pmod{q}, \qquad 1 \le n_1, \ldots, n_k \le q^\beta, \ u \in \mathcal{G},$$

with a multiplicative subgroup $\mathcal{G}$ of $\mathbb{Z}_q^*$. This follows since $q_p(u) = 0$ if $u = r^p$ for some r with $\gcd(r, p) = 1$. So instead of solving (1) we now have much more flexibility and solve (5) with $q = p^2$ and where $\mathcal{G}$ is the group of p-th powers $\pmod{q}$. We note that $\mathcal{G}$ has order $p - 1 \gg q^{1/2}$. This motivates the following result.

Theorem 2. *For any $\varepsilon > 0$ and a sufficiently large cube-free q, and a multiplicative subgroup $\mathcal{G}$ of $\mathbb{Z}_q^*$ of order $t \gg q^{1/2}$ for any integer a with $\gcd(a, q) = 1$, there is always a solution to the congruence (5) with $k = 9$.*

In particular, Theorem 2 implies:

Corollary 3. *Let $\varepsilon > 0$. Suppose p is a sufficiently large prime and $U \ge p^{1/2e^{1/2}+\varepsilon}$. Then, for any integer a with $\gcd(a, p) = 1$, there is always a solution to the congruence (4) with $k = 9$.*

Our approach can also be used to study the solvability of (1) for almost all reduced residue classes $a \pmod q$ and obtain several more results complementing those of Cilleruelo and Garaev [9] and Garaev [14]. We state one such result as follows.

Theorem 4. *For any $\varepsilon > 0$ and a sufficiently large cube-free q, for all but $o(q)$ integers $a \in \{0, \ldots, q-1\}$ with $\gcd(a, q) = 1$, there is always a solution to the congruence* (1) *with $k = 7$.*

In particular, Theorem 4 implies:

Corollary 5. *For any $\varepsilon > 0$, a sufficiently large prime p and $U \geq p^{1/2e^{1/2}+\varepsilon}$, for all but $o(p)$ integers $a \in \{0, \ldots, p-1\}$ with $\gcd(a, p) = 1$, there is always a solution to the congruence* (4) *with $k = 7$.*

2. Preparations

2.1. **Notation.** Throughout the paper, any implied constants in the symbols O, $\ll$ and $\gg$ may depend on the real parameter $\varepsilon > 0$. We recall that the notations $U = O(V)$, $U \ll V$ and $V \gg U$ are all equivalent to the statement that the inequality $|U| \leq cV$ holds with some constant $c > 0$.

We define the constants $\psi = 2^{1/36}$, $\xi = \psi - 1$, and for a real A and an integer a, write $a \sim A$ to indicate $a \in [A, \psi A]$. We also write $\rho = e^{-1/2}$.

We use $\mathbb{Z}_q^*$ to denote the unit group of the residue ring modulo q.

As usual, we write $\varphi(n)$ for the Euler function and $\tau(n)$ to represent the number of positive integer divisors of an integer $n \geq 1$ for which we recall the following well-known estimates

$$(6) \qquad \tau(q) = q^{o(1)} \qquad \text{and} \qquad q \geq \varphi(q) \gg \frac{q}{\log \log q}$$

as $q \to \infty$, see [18, Theorems 317 and 328].

In the following κ always denotes the ratio

$$\kappa = \frac{\varphi(q)}{q}.$$

2.2. **Some basic results.** The next result is a well-known elementary consequence of the identity

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

Lemma 6. *For any $M \geq 1, q \geq 2$ we have*

$$\sum_{\substack{m \sim M \\ \gcd(m,q)=1}} 1 = \xi M \kappa + O(\tau(q)).$$

When M is small in relation to q it is useful to have the following result.

Lemma 7. *For $q \geq 2, M > \log q$ we have*

$$\sum_{\substack{m \sim M \\ \gcd(m,q)=1}} 1 = O(M\kappa) \,.$$

Here the implied constant is absolute.

Proof. This follows from [17, Theorem 2.2]. $\square$

Combining the above results enables us to establish a result which is needed in Subsection 2.3.

Lemma 8. *For $N \geq q^{1/4} > 1, 0 < \zeta < 1$ we have*

$$\sum_{\substack{N^\zeta \leq p \leq N \\ \gcd(p,q)=1}} \sum_{\substack{m \sim N/p \\ \gcd(m,q)=1}} 1 = (\xi \log(1/\zeta) + o(1))\kappa N \,.$$

Proof. From Lemmas 6 and 7 together with a trivial bound we have

$$\sum_{\substack{m \sim N/p \\ \gcd(m,q)=1}} 1 = \xi N \kappa p^{-1} + O(\vartheta_p)$$

where

$$(7) \qquad \vartheta_p = \begin{cases} \tau(q) & \text{if } p < N/\tau(q), \\ \kappa N/p & \text{if } N/\tau(q) \leq p \leq N/\log q, \\ N/p & \text{if } p > N/\log q. \end{cases}$$

(note the ranges may partially overlap and the second range may be empty). By the Mertens formula, see [22, Equation (2.15)], for any real $Y > X \geq 2$ we have

$$\sum_{X \leq p \leq Y} \frac{1}{p} = \log \frac{\log Y}{\log X} + O\left(\frac{1}{\log X}\right).$$

Hence

$$\sum_{\substack{N^\zeta \leq p \leq N \\ \gcd(p,q)=1}} \xi N \kappa p^{-1} = (\xi \log(1/\zeta) + o(1))\kappa N$$

gives us the main term (where we have also noted that there are only $O(1)$ primes $p \mid q$ with $p > N^\zeta$).

For the error term we consider the 3 possible ranges in (7) separately.

For the first range, by Prime Number Theorem and the bound

$$\kappa \gg \frac{1}{\log \log q},$$

see (6), we derive

$$\sum_{p<N/\tau(q)} \vartheta_p \ll \sum_{p<N/\tau(q)} \tau(q) = (1+o(1))\frac{N}{\log N} = o(\kappa N).$$

For the second range (provided it is not empty) using the above Mertens formula and (6), we obtain

$$\sum_{N/\tau(q)\leq p\leq N/\log q} \vartheta_p \ll \kappa N \sum_{N/\tau(q)\leq p\leq N/\log q} \frac{1}{p}$$

$$= \kappa N \left(\log \frac{\log N - \log\log q}{\log N - \log\tau(q)} + O\left(\frac{1}{\log N}\right) \right)$$

$$= \kappa N \left(\log \frac{\log N + o(\log N)}{\log N + o(\log N)} + O\left(\frac{1}{\log N}\right) \right)$$

$$= \kappa N \left(\log(1+o(1)) + O\left(\frac{1}{\log N}\right) \right) = o(\kappa N).$$

Finally, for the third range, similarly, we have

$$\sum_{N/\log q<p\leq N} \vartheta_p \ll N \sum_{N/\log q<p\leq N} \frac{1}{p}$$

$$= N \left(\log \frac{\log N}{\log N - \log\log q} + O\left(\frac{1}{\log N}\right) \right)$$

$$= N \left(\log \frac{\log N}{\log N + O(\log\log N)} + O\left(\frac{1}{\log N}\right) \right)$$

$$\ll N \frac{\log\log N}{\log N} = o(\kappa N).$$

The desired result now follows. $\qquad\qquad\square$

2.3. **Using a simple idea of Balog.** Instead of establishing a variant of [19, Lemma 1] which uses an idea of Friedlander [12] to obtain a lower bound of the correct order of magnitude for the integers we wish to count, we return to the original idea of Balog [1]. That is, we count products of two numbers mn, and note, for any set $\mathcal{A}$,

$$\sum_{\substack{mn\in\mathcal{A}\\p|mn\Rightarrow p<x^\alpha}} 1 \geq \sum_{\substack{mn\in\mathcal{A}\\p|m\Rightarrow p<x^\alpha}} 1 - \sum_{\substack{mn\in\mathcal{A}\\\exists p|n,p>x^\alpha}} 1.$$

We do this for simplicity as it would take considerable effort to obtain the correct order lower bound in view of the complicated structure we impose on the numbers we have eventually to count. We write for

convenience $\mathcal{B} = \{n : \gcd(n, q) = 1\}$. Our main auxiliary result is then as follows.

Lemma 9. *Suppose $R > N > q^{1/4}$. Let $\varepsilon > 0$ be given and a sequence b_r supported on the interval $[R, \psi^{34}R]$. Suppose that $\mathcal{A} \subseteq \mathcal{B}$ is a set such that for some $\lambda > 0$ and $\eta = \varepsilon^3$,*

$$(8) \qquad \sum_{\substack{rnm\in\mathcal{A} \\ m,n\sim N}} a_n b_r = \lambda \sum_{\substack{rnm\in\mathcal{B} \\ m,n\sim N}} a_n b_r + O(\lambda x^{1-\eta})$$

for any sequence $a_n = O(1)$. Write $\zeta = \rho(1 + \varepsilon)$. Let

$$c_n = \begin{cases} 1 & \text{if } p \mid n \Rightarrow p < N^\zeta \\ 0 & \text{otherwise.} \end{cases}$$

Then

$$(9) \quad \sum_{\substack{rmn\in\mathcal{A} \\ m,n\sim N}} b_r c_n c_m \geq (2 + o(1))\lambda \log(1 + \varepsilon)(\kappa\xi N)^2 \sum_{r\in\mathcal{B}} b_r + O(\lambda x^{1-\eta})\,.$$

Proof. Using the observation of Balog [1], we have

$$\sum_{\substack{rmn\in\mathcal{A} \\ m,n\sim N}} b_r c_n c_m \geq E - F$$

where

$$E = \sum_{\substack{rmn\in\mathcal{A} \\ m,n\sim N}} b_r c_m\,, \qquad F = \sum_{\substack{rmn\in\mathcal{A} \\ m,n\sim N}} b_r h_n\,,$$

and $h_n = 1 - c_n$. By (8)

$$E = \lambda \sum_{\substack{rmn\in\mathcal{B} \\ m,n\sim N}} b_r c_m + O(\lambda x^{1-\eta}).$$

Now

$$\sum_{\substack{rmn\in\mathcal{B} \\ m,n\sim N}} b_r c_m = \sum_{\substack{m\in\mathcal{B} \\ m\sim N}} c_m \sum_{\substack{n\in\mathcal{B} \\ n\sim N}} 1 \sum_{r\in\mathcal{B}} b_r\,.$$

Lemmas 6 and 8 then give

$$\sum_{\substack{n\in\mathcal{B} \\ n\sim N}} 1 = (1 + o(1))\kappa\xi N, \qquad \sum_{\substack{m\in\mathcal{B} \\ m\sim N}} c_m = (1 + \log\zeta + o(1))\kappa\xi N\,,$$

where we have noted (since $\rho > \frac{1}{2}$) that

$$\sum_{\substack{m\in\mathcal{B} \\ m\sim N}} c_m = \sum_{\substack{m\in\mathcal{B} \\ m\sim N}} 1 - \sum_{N^\zeta < p \leq N} \sum_{\substack{m\in\mathcal{B} \\ m\sim N/p}} 1\,.$$

Thus

$$E = \lambda(1 + \log\zeta + o(1))(\kappa\xi N)^2 \sum_{r \in \mathcal{B}} b_r + O(\lambda x^{1-\eta}).$$

Similarly

$$F = \lambda(-\log\zeta + o(1))(\kappa\xi N)^2 \sum_{r \in \mathcal{B}} b_r + O(\lambda x^{1-\eta}).$$

Since $1 + 2\log\zeta = 2\log(1 + \varepsilon)$ we obtain (9). $\square$

Now we define the *multiset*

(10) $\mathcal{K} = \{k = mn \ : \ m, n \sim N, p \mid mn \Rightarrow p < N^\zeta\},$

where the integers k are counted with multiplicity. For a real $x > 1$ and integers a and q with $\gcd(a, q) = 1$ and a subgroup $\mathcal{G}$ of $\mathbb{Z}_q^*$ we define by $\mathcal{A}_{a,q}(\mathcal{G}; x)$ the set of integers $s \in [x, 2x]$ with $s \equiv au \pmod{q}$ for some $u \in \mathcal{G}$. We record a special case of Lemma 9 that applies to the set $\mathcal{A} = \mathcal{A}_{a,q}(\mathcal{G}; x)$.

Corollary 10. *Assume that the conditions of Lemma 9 holds with* $x = N^2 R > x_0(\varepsilon)$ *for the set* $\mathcal{A} = \mathcal{A}_{a,q}(\mathcal{G}; x)$ *with* $\lambda = t/\varphi(q)$, *where* $t = \#\mathcal{G}$ *and* $x_0(\varepsilon)$ *depends only on* ε *and is sufficiently large. Then*

$$\sum_{\substack{rk \in \mathcal{A}_{a,q}(\mathcal{G};x) \\ k \in \mathcal{K}}} b_r \geq \varepsilon \frac{t\kappa^2\xi^2 N^2}{\varphi(q)} \sum_{r \in \mathcal{B}} b_r + O\left(tq^{-1} x^{1-\eta}\right).$$

In particular, for the extreme case $\mathcal{G} = \{1\}$, we write $\mathcal{A}_{a,q}(x)$ for $\mathcal{A}_{a,q}(\{1\}, x)$ and obtain:

Corollary 11. *Assume that the conditions of Lemma 9 holds with* $x = N^2 R > x_0(\varepsilon)$ *for the set* $\mathcal{A} = \mathcal{A}_{a,q}(x)$ *with* $\lambda = 1/\varphi(q)$, *where* $x_0(\varepsilon)$ *depends only on* ε *and is sufficiently large. Then*

$$\sum_{\substack{rk \in \mathcal{A}_{a,q}(x) \\ k \in \mathcal{K}}} b_r \geq \varepsilon \frac{\kappa^2\xi^2 N^2}{\varphi(q)} \sum_{r \in \mathcal{B}} b_r + O\left(q^{-1} x^{1-\eta}\right).$$

2.4. **Character sums.** Let $\mathcal{X}$ be the set of all $\varphi(q)$ multiplicative characters modulo q and let $\mathcal{X}^*$ be the set of nonprincipal characters $\chi \neq \chi_0$. We now recall the Burgess bound for sums of multiplicative characters modulo cube-free integers which we present in the following simplified form, see [22, Theorems 12.5 and 12.6].

Lemma 12. *There is an absolute constant $c > 0$ such that for any fixed $\delta \in (0, 1/2)$, a cube-free integer q and an arbitrary integer $M \geq q^{1/4+\delta}$,*

for any $\chi \in \mathcal{X}^*$ we have

$$\left| \sum_{m \leq M} \chi(m) \right| \ll M^{1-c\delta^2}.$$

Finally, we need the following simple bound which follows from the orthogonality of characters and which we refer to as the *mean-value estimate for character sums.*

Lemma 13. *For $N \geq 1$ and any sequence of complex numbers a_n we have*

$$\sum_{\chi \in \mathcal{X}} \left| \sum_{n \leq N} a_n \chi(n) \right|^2 \leq \varphi(q)(N/q + 1) \sum_{n \leq N} |a_n|^2.$$

2.5. **Products in arithmetic progressions.** We now define

(11) $\qquad \delta = 1/200 \qquad$ and $\qquad \alpha = \left(\frac{1}{4} + \varepsilon \right) \left(2 + \delta + 2\varepsilon \right)^{-1}.$

For a given q, we consider the set of integers r that are products of 33 primes of the form

(12) $\qquad r = \ell_1 \ldots \ell_{21} p_1 \ldots p_8 s_1 \ldots s_4 \qquad$ and $\qquad \gcd(r, q) = 1,$

where

(13) $\qquad \ell_1, \ldots, \ell_{21} \sim q^\delta, \quad p_1, \ldots, p_8 \sim q^{3/20}, \quad s_1, s_2, s_3, s_4 \sim q^{1/20},$

and let b_r be the characteristic function of this set. We note that b_r is supported on the interval $[R, \psi^{33}R]$ with $R = q^{3/2+\delta}$.

We now show that for any sufficiently small $\varepsilon > 0$ the conditions of Lemma 9 are satisfied for this choice of b_r with $N = q^{1/4+\varepsilon} = x^\alpha$ upon writing $x = N^2R$.

Lemma 14. *Let $\varepsilon > 0$ be sufficiently small, $q > 1$ and $N = q^{1/4+\varepsilon}$. Suppose that the sequence b_r is the characteristic function of the set defined by (12) and (13). Then for integers a and q with $\gcd(a, q) = 1$ and such that q is cube-free we have*

$$\sum_{\substack{rmn \in \mathcal{A}_{a,q}(x) \\ m,n \sim N}} a_n b_r = \frac{1}{\varphi(q)} \sum_{\substack{rmn \in \mathcal{B} \\ m,n \sim N}} a_n b_r + O\left(q^{-1} x^{1-\eta} \right)$$

with $\eta = \varepsilon^3$, $R = q^{3/2+\delta}$ and $x = N^2R$, and any sequence a_n satisfying $|a_n| \leq n^{o(1)}$.

Proof. We start with the observation that if $b_r \neq 0$ and $m, n \sim N$ then due to the choice of our parameters we always have

$$rmn \in [N^2R, \psi^{33}N^2R] \subset [x, 2x].$$

In particular, if $b_r \neq 0$ and $m, n \sim N$ then the condition $rmn \in \mathcal{A}_{a,q}(x)$ is equivalent to the congruence $rmn \equiv a \pmod{q}$ and the condition $rmn \in \mathcal{B}$ is merely equivalent to $\gcd(mn, q) = 1$.

Using the orthogonality of characters we write

$$\sum_{\substack{rmn \in \mathcal{A}_{a,q}(x) \\ m,n \sim N}} a_n b_r = \sum_{\substack{rmn \in \mathcal{B} \\ m,n \sim N}} a_n b_r \frac{1}{\varphi(q)} \sum_{\chi \in \mathcal{X}} \chi(rmna^{-1}).$$

Changing the order of summation, we obtain the asymptotic formula

$$(14) \qquad \sum_{\substack{rmn \in \mathcal{A}_{a,q}(x) \\ m,n \sim N}} a_n b_r = \mathfrak{M} + O\left(\mathfrak{E}\right),$$

where the main term

$$(15) \qquad \mathfrak{M} = \frac{1}{\varphi(q)} \sum_{\substack{rmn \in \mathcal{B} \\ m,n \sim N}} a_n b_r$$

comes from the contribution of the principal character χ_0 and the error term is given by

$$\mathfrak{E} = \frac{1}{\varphi(q)} \sum_{\chi \in \mathcal{X}^*} \left| \sum_{\substack{rmn \in \mathcal{B} \\ m,n \sim N}} a_n b_r \chi(rmn) \right| = \frac{1}{\varphi(q)} \sum_{\chi \in \mathcal{X}^*} \left| \sum_{\substack{r \in \mathcal{R} \\ m,n \sim N}} a_n b_r \chi(rmn) \right|,$$

where $\mathcal{R}$ is the set of r defined by (12) and (13) (note that due to the presence of characters the condition $rmn \in \mathcal{B}$ can now be dropped).

Hence

$$(16) \qquad \mathfrak{E} = \frac{1}{\varphi(q)} \sum_{\chi \in \mathcal{X}^*} \left| \sum_{m \sim N} \chi(m) \right| \left| \sum_{r \in \mathcal{R}} \sum_{n \sim N} a_n b_r \chi(rn) \right|.$$

We now use the argument deployed in [14], we however put it in a different form which optimally extracts all available information about the character sums involved (thus in case the bound on error terms is important it leads to stronger estimates). This approach also seems to be more direct and since it may have some other applications, we present it in full detail.

For a real $\omega > 0$ we consider the character sums over primes

$$V_\omega(\chi) = \sum_{\ell \sim q^\omega} \chi(\ell).$$

which we use with $\omega = 3/20$ and $\omega = \delta$. We also consider the weighted sums

$$W(\chi) = \sum_{m \sim N} \sum_{n \sim N} \sum_{v \in \mathcal{V}} a_n \chi(mnv),$$

where v runs through the set $\mathcal{V}$ of $q^{1/2+o(1)}$ products $v = p_7 p_8 s_1 s_2 s_3 s_4$ over all $p_7, p_8, s_1.s_2, s_3, s_4$ as in (12). Recalling the definition of b_r, we write (16) as

$$(17) \qquad \mathfrak{E} = \frac{1}{\varphi(q)} \sum_{\chi \in \mathcal{X}^*} \left| V_{3/20}(\chi) \right|^6 \left| V_\delta(\chi) \right|^{21} \left| W(\chi) \right|.$$

We now note that the currently available information about the sums $V_{3/20}(\chi)$, $V_\delta(\chi)$, and $W(\chi)$ consists of the inequality

$$(18) \qquad \max_{\chi \in \mathcal{X}^*} |W(\chi)| \le N^{1+o(1)} q^{1/2} \max_{\chi \in \mathcal{X}^*} \left| \sum_{m \sim N} \chi(m) \right| \ll N^{2 - c_0 \varepsilon^2} q^{1/2}$$

with some absolute constant $c_0 > 0$ for all sufficiently small $\varepsilon > 0$ that follows from Lemma 12 and also the inequalities

$$(19) \qquad \sum_{\chi \in \mathcal{X}} \left| V_{3/20}(\chi) \right|^{12} \left| V_\delta(\chi) \right|^{40} \ll q^2, \qquad \sum_{\chi \in \mathcal{X}} |V_\delta(\chi)|^{400} \ll q^2,$$

and

$$(20) \qquad \sum_{\chi \in \mathcal{X}} \left| \sum_{m \sim N} \sum_{n \sim N} a_n \sum_{v \in \mathcal{V}} \chi(mnv) \right|^2$$
$$\ll N^2 q^{3/2 + o(1)} \left(1 + N^2 q^{-1/2} \right),$$

implied by Lemma 13. Since for the above choice of parameters we have $N^2 > q^{1/2}$, the inequality (20) simplifies as

$$(21) \qquad \sum_{\chi \in \mathcal{X}} \left| \sum_{m \sim N} \sum_{n \sim N} a_n \sum_{v \in \mathcal{V}} \chi(mnv) \right|^2 \ll N^4 q^{1+o(1)}.$$

We now write $|W(\chi)| = |W(\chi)|^{199/200} |W(\chi)|^{1/200}$ and apply (18), deriving from (17)

$$(22) \qquad \mathfrak{E} \le \frac{1}{\varphi(q)} \left(N^{2 - c_0 \varepsilon^2} q^{1/2} \right)^{1/200} \sum_{\chi \in \mathcal{X}^*} \left| V_{3/20}(\chi) \right|^6$$
$$\left| V_\delta(\chi) \right|^{21} |W(\chi)|^{199/200}.$$

Finally, since

$$\frac{1}{2} + \frac{1}{400} + \frac{1}{400/199} = 1$$

by the Hölder inequality, applied to the sum in (22), and extending the summation to all $\chi \in \mathcal{X}$, we obtain

$$\mathfrak{E} \le \frac{1}{\varphi(q)} \left(N^{2-c_0\varepsilon^2} q^{1/2} \right)^{1/200} \left(\sum_{\chi \in \mathcal{X}} \left| V_{3/20}(\chi) \right|^{12} \left| V_\delta(\chi) \right|^{40} \right)^{1/2}$$

$$\left(\sum_{\chi \in \mathcal{X}} \left| V_\delta(\chi) \right|^{400} \right)^{1/400} \left(\sum_{\chi \in \mathcal{X}} \left| W(\chi) \right|^2 \right)^{199/400}.$$

Recalling (19) and (21), we derive

$$(23) \qquad \begin{aligned} \mathfrak{E} &\le \frac{1}{\varphi(q)} \left(N^{2-c_0\varepsilon^2} q^{1/2} \right)^{1/200} q^{1+1/200} \left(N^4 q^{1+o(1)} \right)^{199/400} \\ &\le N^2 q^{1/2+\delta+o(1)} N^{-c_0\varepsilon^2/200} = x q^{-1} N^{-c_0\varepsilon^2/200+o(1)}. \end{aligned}$$

The proof is completed by combining (15) and (23) with (14). $\qquad \square$

2.6. **Products in subgroups.** Before embarking on the proof of Theorem 2 we also require one additional result, that gives an upper bound on the number of solutions to the congruence

$$(24) \qquad xu \equiv y \pmod{q} \qquad 1 \le x, y \le X, \ u \in \mathcal{G},$$

with a multiplicative subgroup $\mathcal{G}$ of $\mathbb{Z}_q^*$, which is given in [23, Corollary 7.9]. We note that in [23] only the case of a prime modulus $q = p$ is considered, but it is easy to check that the argument works for any integer $q \ge 1$.

Lemma 15. *Given a multiplicative subgroup $\mathcal{G}$ of $\mathbb{Z}_q^*$ with order t satisfying $t \gg q^{1/3}$ and an integer $X \ge q^{3/4} t^{-1/4}$, the number of solutions to the congruence (24) is at most $X^2 t q^{-1+o(1)}$.*

We also recall that several more bounds on the number of solutions to (24) are given in [3, Theorem 1].

We replace (11) to define δ and α now with

$$\delta = 1/200 \qquad \text{and} \qquad \alpha = (\tfrac{1}{4} + \varepsilon)(\tfrac{5}{4} + \delta + 2\varepsilon)^{-1}.$$

For a given q, we consider the set of integers r that are products of 28 primes of the form

$$(25) \qquad r = \ell_1 \dots \ell_{21} p_1 p_2 p_3 s_1 s_2 s_3 s_4 \qquad \text{and} \qquad \gcd(r, q) = 1,$$

where

$$(26) \qquad \ell_1, \dots, \ell_{21} \sim q^\delta, \quad p_1, p_2, p_3 \sim q^{3/20}, \quad s_1, s_2, s_3, s_4 \sim q^{1/20},$$

and let b_r be the characteristic function of this set. We remark that we need r to be expressible as two factors of size about $q^{3/8}$ as well as having the right combinatorial properties for our final argument.

Lemma 16. *Let $\varepsilon > 0$ be sufficiently small, $q > 1$ and $N = q^{1/4+\varepsilon}$. Suppose that the sequence b_r is the characteristic function of the set defined by (25) and (26). Then for integers a and q with $\gcd(a,q) = 1$ and such that q is cube-free and a subgroup $\mathcal{G} \subseteq \mathbb{Z}_q^*$ of order $t \gg q^{1/2}$ we have*

$$\sum_{\substack{rmn \in \mathcal{A}_{a,q}(\mathcal{G};x) \\ m,n \sim N}} a_n b_r = \frac{t}{\varphi(q)} \sum_{\substack{rmn \in \mathcal{B} \\ m,n \sim N}} a_n b_r + O\left(tq^{-1}x^{1-\eta}\right)$$

with $\eta = \varepsilon^3$, $R = q^{3/4+\delta}$ and $x = N^2 R$, and any sequence a_n satisfying $|a_n| \le n^{o(1)}$.

Proof. We proceed as in the proof of Lemma 14. We note that we count each desired solution t times by considering

$$mnr \equiv auv \pmod{q},$$

where

$$r \text{ as in } (26), \qquad m \sim N, \qquad n \sim N, \qquad u, v \in \mathcal{G}.$$

As before in the proof of Lemma 14 we use multiplicative characters to obtain a main term

$$(27) \qquad \mathfrak{M} = \frac{t^2}{\varphi(q)} \sum_{\substack{rmn \in \mathcal{B} \\ m,n \sim N}} a_n b_r$$

for the corresponding sum, which we write as

$$\sum_{\substack{mnr \equiv auv \pmod{q} \\ m,n \sim N \\ u,v \in \mathcal{G}}} a_n b_r = \mathfrak{M} + O(\mathfrak{E}).$$

We also write

$$V_\delta(\chi) = \sum_{\ell \sim q^\delta} \chi(\ell),$$

$$W_1(\chi) = \sum_{m \sim N} \sum_{p_1,p_2} \sum_{s_1} \sum_{\ell_1,\ldots,\ell_5} \sum_{u \in \mathcal{G}} \chi(mp_1p_2s_1\ell_1 \ldots \ell_5\overline{u}),$$

$$W_2(\chi) = \sum_{n \sim N} \sum_{p_3} \sum_{s_2,s_3,s_4} \sum_{\ell_6,\ldots,\ell_{20}} \sum_{v \in \mathcal{G}} a_n \chi(np_3s_2s_3s_4\ell_6 \ldots \ell_{20}\overline{v}).$$

So the expression for the error term $\mathfrak{E}$ corresponding to (16) is now

$$\mathfrak{E} = \frac{1}{\varphi(q)} \sum_{\chi \in \mathcal{X}^*} |V_\delta(\chi)| \, |W_1(\chi)| \, |W_2(\chi)| \, .$$

Working in a similar manner to previously we estimate this as

$$\mathfrak{E} \leq \max_{\chi \in \mathcal{X}^*} |W_1(\chi)|^\delta \left(\frac{1}{\varphi(q)} \sum_{\chi \in \mathcal{X}} |V_\delta(\chi)|^{400} \right)^{1/400} S_1^{199/400} S_2^{1/2},$$

where

$$S_j = \frac{1}{\varphi(q)} \sum_{\chi \in \mathcal{X}} |W_j(\chi)|^2 \, .$$

From Lemma 12, we have, for $\chi \in \mathcal{X}^*$,

$$|W_1(\chi)| \leq N^{1-c_0\varepsilon^2} tZ,$$

where Z is the maximum number of all admissible products of the form $p_1 p_2 s_1 \ell_1 \ldots \ell_5$ satisfying (26), so

(28) $$Z \ll q^{3/10+1/20+1/40} = q^{3/8}.$$

This and (19) imply the bound

(29) $$\mathfrak{E} \leq \left(N^{1-c_0\varepsilon^2} t q^{3/8} \right)^\delta q^{\delta/2} S_1^{199/400} S_2^{1/2}.$$

Also, we can estimate S_1 as $S_1 \leq R q^{o(1)}$ where R is the number of solutions to the congruence

$$m_1 p_1 p_2 s_1 \ell_1 \ldots \ell_5 u \equiv m_2 p_3 p_4 s_2 \ell_6 \ldots \ell_{10} v \pmod{q},$$

where

$$p_j, s_j, \ell_j \text{ are as in (26)}, \qquad m_1, m_2 \sim N, \qquad u, v \in \mathcal{G} \, .$$

Now $R \ll tQ$ where Q is the number of solutions to (24) with

$$X \ll NZ \ll X,$$

where Z is given by (28). As $t \geq q^{1/2}$ and $N > q^{1/4}$, we have

$$NZ \gg N q^{3/8} \geq q^{5/8} \geq q^{3/4} t^{-1/4}.$$

Hence Lemma 15 applies and we obtain

$$Q \leq (NZ)^2 t q^{-1+o(1)} = N^2 t q^{-1/4+o(1)}.$$

We also proceed similarly for S_2. Hence

(30) $$S_1 \leq N^2 t^2 q^{-1/4+o(1)} \qquad \text{and} \qquad S_2 \leq N^2 t^2 q^{-1/4+o(1)}.$$

We can now substitute the estimates (30) in (29), to deduce that

$$\mathfrak{E} \leq \left(N^{1-c_0\varepsilon^2}tq^{3/8}\right)^{\delta} q^{\delta/2} \left(N^2t^2q^{-1/4+o(1)}\right)^{(1-\delta)/2} \left(N^2t^2q^{-1/4+o(1)}\right)^{1/2}$$

$$\leq N^2t^2q^{-1/4+\delta+o(1)}N^{-c_0\delta\varepsilon^2}.$$

Hence

$$(31) \qquad \mathfrak{E} \leq xt^2q^{-1}M^{-c_0\varepsilon^2/200+o(1)}.$$

The proof is completed by combining (27) and (31) upon recalling that we are counting each solution t times. $\qquad\square$

3. PROOFS OF MAIN RESULTS

3.1. **Proof of Theorem 1.** We fix some sufficiently small $\varepsilon > 0$. Let α and δ be as in (11) and let η be as in Corollary 11. We also choose x as in Lemma 14. We remark that $N^{\zeta} < x^{\beta+\varepsilon}$.

For integers a and q with $\gcd(a,q) = 1$ and such that q is cube-free we consider the number T of solutions to the congruence

$$(32) \qquad rk \equiv a \pmod{q}$$

where r is defined by (12) and (13) and $k \in \mathcal{K}$, where the multiset $\mathcal{K}$ is defined by (10).

Combining Corollary 11 and Lemma 14, we see that

$$(33) \qquad T = \sum_{\substack{rk \in \mathcal{A}_{a,q}(x) \\ k \in \mathcal{K}}} b_r \geq \varepsilon \frac{\kappa^2 \xi^2 N^2}{\varphi(q)} \sum_{r \in \mathcal{B}} b_r + O\left(q^{-1}x^{1-\eta}\right).$$

By the prime number theorem there are $q^{3/2+\delta+o(1)}$ values of r given by (12) and (13) and for each of them $q^{3/2+\delta} \ll r \ll q^{3/2+\delta}$. Hence, for a sufficiently small $\varepsilon > 0$, after simple calculations, we obtain

$$T \geq xq^{-1+o(1)}.$$

In particular, $T > 0$. Let (k,r) be one of the solutions to (32). Clearly r has 8 prime factors of size $q^{3/20} < q^{\beta+\varepsilon}$. We return to the other 25 factors after an initial discussion of m and n showing that they are both products of at most 3 integer factors of size at most $u = q^{\beta+\varepsilon}$. Indeed, let $\widetilde{p}_1 \geq \ldots \geq \widetilde{p}_{\nu}$ be prime divisors of m. Define h by the condition

$$\widetilde{p}_1 \ldots \widetilde{p}_h \leq u < \widetilde{p}_1 \ldots \widetilde{p}_h \widetilde{p}_{h+1}.$$

Then for

$$v_1 = \widetilde{p}_1 \ldots \widetilde{p}_h, \qquad v_2 = \widetilde{p}_{h+1}, \qquad v_3 = \frac{n}{v_1 v_2}$$

we obviously have $v_1 v_2 v_3 = m$ and also

$$\max\{v_1, v_2, v_3\} \leq \max\{u, u, m/u\} \leq u,$$

provided that $\varepsilon > 0$ is sufficiently small. In particular, in what follows, we always assume that

$$\varepsilon < \frac{1}{2}\delta.$$

Now, clearly $\min\{v_1, v_2, v_3\} \le m^{1/3} < q^{(1+\delta)/12}$. For convenience, suppose that $v_1 \ge v_2 \ge v_3$. So, if $v_2 > q^{1/10}$ then $v_3 < q^{1/20+\delta/4}$. Hence we can combine s_1 and s_2 with v_2 and v_3 to produce new variables not exceeding $q^{3/20+\delta/4}$. So we have written $ms_1s_2 = g_1g_2g_3$ say with each positive integer $g_j \le q^{\beta+\varepsilon}$. However,

$$g_1g_2g_3\ell_1\ldots\ell_{11} \le q^{2/5+5\delta/4},$$

So, suppose $g_j \le q^{3/20-\delta}$. We can include variables $\ell_1, \ldots \ell_h$ so that

$$q^{3/20-\delta} \le g_j\ell_1\ldots\ell_h \le q^{3/20}.$$

We can do this for each $g_j \le q^{3/20-\delta}$ and since, for a sufficiently large q, we have

$$g_1g_2g_3\ell_1\ldots\ell_{11} \le q^{2/5+5\delta/4} < \psi^{-3}q^{3\times 3/20-3\delta}$$
$$\le q^{3\times 3/20}\left(\max\{\ell \sim q^\delta\}\right)^{-3}$$

we use up all $\ell_1, \ldots, \ell_{11}$. In this way $ms_1s_2\ell_1\ldots\ell_{11}$ has been expressed as the product of three variables not exceeding $q^{\beta+\varepsilon}$.

The same argument also applies to n, although in this case we need only use 10 of the ℓ_j variables. We have thus reduced our product to 14 variables as desired.

3.2. **Proof of Theorem 2.** We now proceed as in the proof of Theorem 1 by using Lemma 16 instead of Lemma 14 and applying Corollary 10. We have 3 variables of the correct shape immediately in p_1, p_2, p_3. We can use the same argument as before to reduce $\ell_1\ldots\ell_{21}s_1\ldots s_4mn$ to a product of 6 variables not exceeding $q^{\beta+\varepsilon}$. This gives the 9 variables as required.

3.3. **Proof of Theorem 4.** Suppose that $\mathcal{R}$ is the set of multiplicative inverses $(\bmod\, q)$ of the exceptional set of a. All we need do is prove that for any set $\mathcal{R}$ with $|\mathcal{R}| = q^{1+o(1)}$ there is a solution to

$$rn_1\ldots n_7 \equiv 1 \pmod{q}, \quad 1 \le n_1, \ldots, n_7 \le q^{\beta+\varepsilon}, \ r \in \mathcal{R}.$$

To modify the proof of Theorem 1 we keep the definiton of α, δ from (11) and we initially solve

$$rmnps_1s_2s_3s_4\ell_1\ldots\ell_{31} \equiv 1 \pmod{q},$$
$$\ell_1, \ldots, \ell_{31} \sim q^\delta \qquad p \sim q^{3/20}, \qquad s_1, s_2, s_3, s_4 \sim q^{1/20}.$$

As before $mns_1s_2s_3s_4 = g_1 \ldots g_6$ with each $g_j \le q^{\beta+\varepsilon}$. Now

$$g_1 \ldots g_6 \ell_1 \ldots \ell_{31} \le q^{17/20+5\delta/4} < \psi^{-6} q^{6\times 3/20 - 6\delta}$$

$$\le q^{6\times 3/20} \left(\max\{\ell \sim q^\delta\}\right)^{-6}.$$

We can therefore combine some of the ℓ_j variables with each g_k in turn to obtain 6 new variables not exceeding $g_j \le q^{\beta+\varepsilon}$. We thus end up with 7 variables of the required form as desired.

4. ADDITIONAL RESULTS

A natural question is to see how far short our results fall from what would be known assuming the Generalised Riemann Hypothesis. Under that assumption we quickly obtain the well-known conditional bound for a short sum over a non-principal multiplicative character χ modulo q:

$$(34) \qquad \sum_{m \le M} \chi(m) \ll M^{1/2} q^{o(1)},$$

as $q \to \infty$, see [25, Section 1]; it can also be derived from [16, Theorem 2].

We also obtain the following conditional extension of Theorem 2 without any need to use Lemma 9, where as usual we use $\lfloor x \rfloor$ to denote the integer part of real x.

Theorem 17. *Assume the Generalised Riemann Hypothesis. For any $\beta \in (0,1)$ and a sufficiently large q, a multiplicative subgroup $\mathcal{G}$ of $\mathbb{Z}_q^*$ of order $t = q^\vartheta$, for any integer a with $\gcd(a,q) = 1$, there is always a solution to the congruence (5) with $k = \lfloor 2(1-\vartheta)/\beta \rfloor + 1$.*

Proof. Since $\mathcal{G}$ is a group, for fixed u the number of solutions to $vw = u$ with $v, w \in \mathcal{G}$ is t. Hence the number of solutions to (5) is $t^{-1}S$ where S is the number of solutions to

$$n_1 \ldots n_k \equiv avw \pmod{q}, \qquad 1 \le n_1, \ldots, n_k \le q^\beta, \ v, w \in \mathcal{G}.$$

Using character sums we obtain $S = M + O(E)$ where

$$\frac{M}{t^2} = \frac{1}{\varphi(q)} \left(\sum_{n \le q^\beta} \chi_0(n)\right)^k = q^{k\beta - k}\varphi(q)^{k-1} + O\left(q^{(k-1)\beta - 1 + o(1)}\right),$$

and

$$E = \frac{1}{\varphi(q)} \sum_{\chi \ne \chi_0} \left|\sum_{n \le q^\beta} \chi(n)\right|^k \left|\sum_{u \in \mathcal{G}} \chi(u)\right|^2.$$

Using (34) applied to the sum over n and the mean value theorem for character sums for the sum of the sums over u gives

$$E \leq q^{k\beta/2+o(1)}t.$$

We thus obtain that the number of solutions to (5) is

$$S/t = tq^{k\beta-k}\varphi(q)^{k-1} + O\left(tq^{(k-1)\beta-1+o(1)} + q^{k\beta/2+o(1)}\right).$$

Hence $S > 0$ for q sufficiently large when

$$k\beta - 1 > (k-1)\beta - 1 \qquad \text{and} \qquad \vartheta + k\beta - 1 > k\beta/2.$$

The first inequality is always satisfied as $\beta > 0$, analysing the second inequality we obtain the result. $\square$

Comparing this (taking $\mathcal{G}$ to be the trivial subgroup) with our unconditional result we see that for $\beta = 1/4e^{1/2}$ we make no saving on the number of variables. However, we can reduce β to $1/7 + \varepsilon$ and still only require 14 variables. The real benefit, of course, is that we can take any $\beta > 0$ to obtain factors essentially as small as we wish. The major constraint imposed by this approach is that the product of the variables must be of size at least $q^{2+\varepsilon}$.

Now let $\mathcal{G}$ be the group of pth powers modulo p^2 as in the proof of Theorem 2. We immediately deduce the following result which saves 2 variables on Theorem 2 for $\beta = 1/4e^{1/2}$.

Corollary 18. *Assume the Generalised Riemann Hypothesis. For any* $\beta \in (0, 1/2)$ *and a sufficiently large prime* p *for any integer* a *with* $\gcd(a, p) = 1$ *and* $U \geq p^{2\beta}$, *there is always a solution to the congruence* (4) *with* $k = \lfloor 1/\beta \rfloor + 1$.

The next natural question is: what happens for almost all moduli? The auxiliary results used in proving the Bombieri-Vinogradov Theorem (see [10, Chapter 28]) immediately show that Theorem 17 is true for $\mathcal{G} = \{1\}$ unconditionally for all $q \in [Q, 2Q]$ with $o(Q)$ exceptions as well as for almost all prime $p = q \in [Q, 2Q]$ with $o(Q/\log Q)$ exceptions. One can obtain results for non-trivial $\mathcal{G}$, but the results become complicated and do not have the full strength of Theorem 17.

An alternative approach to results for almost all q is via a bound of Garaev [13] of character sums for almost all moduli (which can be used in place of Lemma 12). This approach may lead to stronger results for some group sizes.

Next, we would like a result for almost all p^2 in order to obtain the appropriate version of Corollary 3 for almost all prime squares. This is possible since Matomäki [24] has obtained an analogous version of the Bombieri-Vinogradov theorem for prime-squared moduli. Using the

Type II sum estimates in [24, Section 3], we are able quickly to deduce the following.

Theorem 19. *For any* $\beta \in (0, 1/2)$ *and a sufficiently large* Q, *for all but* $o(Q^{1/2}/\log Q)$ *exceptional prime squares* $p^2 \in [Q, 2Q]$, *for any integer* a *with* $\gcd(a, p) = 1$, *there is a solution to the congruence*

$$n_1 \ldots n_k \equiv a \pmod{p^2}, \qquad 1 \le n_1, \ldots, n_k \le Q^\beta,$$

with $k = \lfloor 2/\beta \rfloor + 1$.

Corollary 20. *For any* $\beta \in (0, 1/2)$ *and a sufficiently large* T, *for all but* $o(T/\log T)$ *exceptional primes* $p \in [T, 2T]$, *and* $U \ge p^{2\beta}$, *for any integer* b *with* $\gcd(b, p) = 1$, *there is always a solution to the congruence* (4) *with* $k = \lfloor 2/\beta \rfloor + 1$.

Of course, for $\beta = 1/4e^{1/2}$ this is worse than our Theorem 2 which is true for all p, but Corollary 20 does hold for *all* $\beta > 0$.

Finally, we mention that a version of Theorem 2, which involves multiplicative subgroups $\mathcal{G}$ of $\mathbb{Z}_{p^2}^*$ of certain sizes is possible via a version of a result of Garaev [13] for almost all prime squares, of the type given in [30, Theorem 8].

5. COMMENTS

We note that the choice of parameters (25) and (26) is optimised for subgroups of order $t = q^{1/2+o(1)}$. The chief reason for this is that our main application to Fermat quotients corresponds to subgroups of this size. However, one can easily obtain a series of other results of the type of Theorem 2 for subgroups of other sizes. Furthermore, for other choices of parameters several other versions of Lemma 15 may be of use. For example, one can use [3, Theorem 1] with other values of ν and also a similar estimate from [9]. Furthermore, for some ranges of q, t and X, one can obtain better estimates via bounds of multiplicative character sums.

ACKNOWLEDGEMENT

REFERENCES

[1] A. Balog, '$p + a$ without large prime factors', *Sém. Théorie des Nombres Bordeaux (1983-84)*, Exposé 3, 1984, 1–5.

[2] J. Bourgain, K. Ford, S. V. Konyagin and I. E. Shparlinski, 'On the divisibility of Fermat quotients', *Michigan Math. J.*, **59** (2010), 313–328.

[3] J. Bourgain, S. V. Konyagin, and I. E. Shparlinski, 'Product sets of rationals, multiplicative translates of subgroups in residue rings, and fixed points of the discrete logarithm', *Int. Math. Res. Not.*, 2008, Article ID rnn 090, 1–29.

[4] D. A. Burgess, 'The distribution of quadratic residues and non-residues', *Mathematika*, **4** (1957), 106–112.

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

[6] M.-C. Chang, 'Short character sums with Fermat quotients', *Acta Arith.*, **152** (2012), 23–38.

[7] Z. X. Chen and A. Winterhof, 'Interpolation of Fermat quotients', *SIAM J. Discr. Math.*, **28** (2014), 1–7.

[8] Z. X. Chen and A. Winterhof, 'Polynomial quotients: Interpolation, value sets and Waring's problem', *Preprint*, 2014 (available from `http://arxiv.org/abs/1402.1913`).

[9] J. Cilleruelo and M. Z. Garaev, 'Congruences involving product of intervals and sets with small multiplicative doubling modulo a prime', *Preprint*, 2014 (available from `http://arxiv.org/abs/1404.5070`).

[10] H. Davenport, *Multiplicative number theory* (2nd edition revised by H. L. Montgomery), Springer-Verlag, New York 1980.

[11] R. Ernvall and T. Metsänkylä, 'On the *p*-divisibility of Fermat quotients', *Math. Comp.*, **66** (1997), 1353–1365.

[12] J. B. Friedlander, 'Integers free from large and small primes', *Proc. London Math. Soc.*, **33** (1976), 565–576.

[13] M. Z. Garaev, 'Character sums in short intervals and the multiplication table modulo a large prime', *Monat. Math.*, **148** (2006), 127–138.

[14] M. Z. Garaev, 'On multiplicative congruences'. *Math. Zeit.* **272** (2012), 473–482.

[15] D. Gomez and A. Winterhof, 'Multiplicative character sums of Fermat quotients and pseudorandom sequences', *Period. Math. Hungarica*, **64** (2012), 161–168.

[16] A. Granville and K. Soundararajan, 'Large character sums' *J. Amer. Math. Soc.*, **14** (2001), 365–397.

[17] H. Halberstam and H.-R. Richert, *Sieve Methods*, Academic Press, New York/London, 1974.

[18] G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers*, Oxford Univ. Press, Oxford, 1979.

[19] G. Harman, 'Integers without large prime factors in short intervals and arithmetic progressions', *Acta Arith.*, **91** (1999), 279–289.

[20] D. Harvey and I. E. Shparlinski, 'Statistics of different reduction types of Fermat curves', *Experimental Math.*, **22** (2013), 243–249.

[21] Y. Ihara, 'On the Euler-Kronecker constants of global fields and primes with small norms', *Algebraic Geometry and Number Theory*, Progress in Math., Vol. 850, Birkhäuser, Boston, Cambridge, MA, 2006, 407–451.

[22] H. Iwaniec and E. Kowalski, *Analytic number theory*, Amer. Math. Soc., Providence, RI, 2004.

[23] S. V. Konyagin and I. E. Shparlinski, *Character sums with exponential functions and their applications*, Cambridge Univ. Press, Cambridge, 1999.

[24] K. Matomäki, 'A note on primes of the form ap^2+1', *Acta Arith.* **137** (2009), 133–137.

[25] H. L. Montgomery and R. C. Vaughan, 'Exponential sums with multiplicative coefficients', *Invent. Math.*, **43** (1977), 69–82.

[26] A. Ostafe and I. E. Shparlinski, 'Pseudorandomness and dynamics of Fermat quotients', *SIAM J. Discr. Math.*, **25** (2011), 50–71.

[27] I. D. Shkredov, 'On Heilbronn's exponential sum', *Quart. J. Math.*, **64** (2013), 1221–1230.

[28] I. E. Shparlinski, 'Character sums with Fermat quotients', *Quart. J. Math.*, **62** (2011), 1031–1043.

[29] I. E. Shparlinski, 'Bounds of multiplicative character sums with Fermat quotients of primes', *Bull. Aust. Math. Soc.*, **83** (2011), 456–462.

[30] I. E. Shparlinski, 'Fermat quotients: Exponential sums, value set and primitive roots', *Bull. Lond. Math. Soc.*, **43** (2011), 1228–1238.

[31] I. E. Shparlinski, 'On the value set of Fermat quotients', *Proc. Amer. Math. Soc.*, **140** (2012), 1199–1206.

[32] I. E. Shparlinski, 'On vanishing Fermat quotients and a bound of the Ihara sum', *Kodai Math. J.*, **36** (2013), 99–108.

DEPARTMENT OF MATHEMATICS, ROYAL HOLLOWAY, UNIVERSITY OF LONDON, EGHAM, SURREY TW20 0EX, UK
E-mail address: `g.harman@rhul.ac.uk`

DEPARTMENT OF PURE MATHEMATICS, UNIVERSITY OF NEW SOUTH WALES, SYDNEY, NSW 2052, AUSTRALIA
E-mail address: `igor.shparlinski@unsw.edu.au`