Mathematika 63 (2017) 483–498 © 2017 University College London
doi:10.1112/S0025579317000043

ON THE LEAST SQUAREFREE NUMBER IN AN ARITHMETIC PROGRESSION

R. M. NUNES

Abstract. We prove an asymptotic formula for squarefree numbers in arithmetic progressions, improving previous results by Prachar and Hooley. As a consequence we improve a lower bound of Heath-Brown for the least squarefree number in an arithmetic progression.

§1. *Introduction.* Let μ denote the Möbius function, i.e. μ is the multiplicative function such that for every prime number p, one has $\mu(p) = -1$ and $\mu(p^j) = 0$ for $j \geqslant 2$. We remark that $\mu^2(n) = 1$ if n is squarefree and $\mu^2(n) = 0$ otherwise. In this paper we are concerned with the distribution of squarefree numbers in arithmetic progressions. By what we just said, this is equivalent to studying the distribution of the μ^2 function in arithmetic progressions.

In this direction, a result of Prachar [6], subsequently improved by Hooley [3], says that

$$\sum_{\substack{n\leqslant X\\ n\equiv a \pmod q}} \mu^2(n) = \frac{1}{\varphi(q)} \sum_{\substack{n\leqslant X\\ (n,q)=1}} \mu^2(n) + O\left(\frac{X^{1/2}}{q^{1/2}} + q^{1/2+\epsilon}\right). \tag{1.1}$$

Here and throughout the article, ϵ denotes a small constant that might vary from line to line and the implied constants in the symbols O and $\ll$ are allowed to depend on ϵ.

It follows from (1.1) that the sequence of squarefree numbers $\leqslant X$ is well distributed in arithmetic progressions modulo q whenever

$$q \leqslant X^{2/3-\epsilon}. \tag{1.2}$$

Even though it is largely believed that one should be able to replace $2/3$ by 1 in the above inequality, this constant has resisted any improvement until very recently.

The author [4] proved, using different techniques than those contained here, that if one restricts to prime values of q, the exponent in (1.2) can be improved to $13/19$. In the present paper we show how to further improve this constant and at the same time relax the condition on q. Our main result is the following.

Received 11 July 2016, published online 23 March 2017.
MSC (2010): 11N37 (primary), 11A07 (secondary).
This work is supported by the DFG-SNF lead agency program grant 200021L-153647.

https://doi.org/10.1112/S0025579317000043 Published online by Cambridge University Press

THEOREM 1.1. *Let $\epsilon > 0$. Then there exists $\delta = \delta(\epsilon) > 0$ such that, uniformly for $X \geqslant 2$, integers a and positive integers q coprime with a satisfying*

$$q \leqslant X^{25/36-\epsilon},$$

we have

$$\sum_{\substack{n\leqslant X\\ n\equiv a \pmod q}} \mu^2(n) = \frac{1}{\varphi(q)} \sum_{\substack{n\leqslant X\\ (n,q)=1}} \mu^2(n) + O\left(\frac{X^{1-\delta}}{q}\right). \tag{1.3}$$

In other terms, the value $\Theta = \frac{25}{36}$ is an exponent of distribution for the characteristic function of the sequence of squarefree numbers μ^2 restricted to squarefree moduli.

Alternatively, one can ask the simpler question of when is the left-hand side of (1.1) non-zero. This amounts to studying the least squarefree number in an arithmetic progression. We let $n(q, a)$ denote the least positive squarefree number which is congruent to a modulo q. Prachar's result implies that

$$n(q, a) \ll q^{3/2+\epsilon}. \tag{1.4}$$

This result was improved by Erdős [1], who essentially proved that $n(q, a) = o(q^{3/2})$, and then later by Heath-Brown [2], who showed the upper bound

$$n(q, a) \ll q^{13/9+\epsilon}. \tag{1.5}$$

It is a direct consequence of Theorem 1.1 that we can also improve this inequality. We have the following.

COROLLARY 1.2. *For every $\epsilon > 0$, uniformly for $(a, q) = 1$, we have the inequality*

$$n(q, a) \ll q^{36/25+\epsilon}.$$

The key input comes from estimates for the number of solutions to a congruence in a dyadic box.

Let q be a positive integer and let $a \in (\mathbb{Z}/q\mathbb{Z})^*$. Let $u > 0$ and v be non-zero integers and let M and N be real numbers such that $M, N \geqslant 1$. We consider the counting function

$$S_{u,v}(M, N, q, a) := \#\{M/2 < m \leqslant M,\ N/2 < n \leqslant N; m^u \equiv an^v \pmod q\},$$

where, if v is negative, we automatically assume that n is invertible modulo q and then n^v stands for $\bar{n}^{|v|}$, where $\bar{n}$ denotes the multiplicative inverse of n modulo q.

It is not hard to deduce the upper bound

$$S_{u,v}(M, N, q, a) \ll \frac{MN}{q} + \min(M, N). \tag{1.6}$$

https://doi.org/10.1112/S0025579317000043 Published online by Cambridge University Press

In certain cases, this can be improved by making use of the Weil bound for exponential sums over curves. For example, suppose that q is squarefree and $(u, v) = 1, u \neq v$. Then we have the inequality

$$S_{u,v}(M, N, q, a) \ll q^{\epsilon}(MNq^{-1} + Mq^{-1/2} + Nq^{-1/2} + q^{1/2}). \tag{1.7}$$

If one is interested in extending the above inequality to non-squarefree moduli, one needs a careful analysis of certain exponential sums modulo a power of a prime. This is elementary but rather tedious, so we are glad that in the case of interest to us, this was already done by Heath-Brown [2].

LEMMA 1.3. *Let q be a positive integer. Then we have, uniformly for $a \in (\mathbb{Z}/q\mathbb{Z})^*$, $1 \leqslant M < q/2$, the inequality*

$$S_{1,-2}(M, N, q, a) \ll (q^{1/2} + MNq^{-1} + Nq^{-1/2})q^{\varepsilon}.$$

This follows from [2, equation (17)], since one can check that his definition of $U(w, M, q, a)$ (see [2, p. 209]) satisfies

$$S(M, N; q, a) \leqslant U(N, M, q, a).$$

Unfortunately, when $M \asymp N \asymp q^{1/2}$, both (1.6) an (1.7) give the same bound

$$S_{u,v}(M, N, q, a) \ll q^{1/2+\epsilon}. \tag{1.8}$$

This is an important threshold when trying to improve (1.1) or (1.4). Indeed, one of the main achievements in [2] is giving an upper bound for $S_{1,-2}(M, N, q, a)$ that improves on (1.8) in the range where $M \asymp N \asymp q^{1/2}$.

The following lemma was proved in [5] in the case where q is squarefree. In the present paper we need to prove it for another family of moduli. Precisely, we need the case where q is the square of a prime.

LEMMA 1.4. *Suppose that q is either squarefree or the square of a prime. Then we have, uniformly for $a \in (\mathbb{Z}/q\mathbb{Z})^*$, $1 \leqslant M \leqslant q^{3/4}$ and $1 \leqslant N < q/2$, the inequality*

$$S_{u,v}(M, N, q, a) \ll M^{2/3}N^{1/4}q^{\varepsilon}.$$

Notice that Lemma 1.4 is more useful when M is small compared to N. In the opposite case, where M is the larger variable, we use the following simple relation:

$$S_{u,v}(M, N, q, a) = S_{-v,-u}(N, M, q, a). \tag{1.9}$$

We will use Lemma 1.4 with $(u, v) = (1, -2)$ and $(u, v) = (2, -1)$. For the first of these pairs, this is contained in the work of Heath-Brown, for both squarefree moduli and squares of primes. For the other pair, the argument in [2] does not transpose directly, and we need to implement some of the novelties contained in [5].

https://doi.org/10.1112/S0025579317000043 Published online by Cambridge University Press

At many steps in the proof of Lemma 1.4 we will need to estimate the number of roots of a polynomial modulo p^2 for a certain prime p, for which we will need Hensel's lemma. We recall that Hensel's lemma says that if $\alpha \in \mathbb{Z}/p\mathbb{Z}$ satisfies

$$P(\alpha) \equiv 0 \pmod{p} \quad \text{and} \quad P'(\alpha) \not\equiv 0 \pmod{p},$$

then there exists a unique $\beta \in \mathbb{Z}/p^2\mathbb{Z}$ such that

$$P(\beta) \equiv 0 \pmod{p^2} \quad \text{and} \quad \beta \equiv \alpha \pmod{p}.$$

As an application of Hensel's lemma, we have the following result that we record here for easier reference.

LEMMA 1.5. *Let $u \neq 0$ be an integer, let p be a prime and $y \in (\mathbb{Z}/p^2\mathbb{Z})^*$. Then the number of solutions for $x \in \mathbb{Z}/p^2\mathbb{Z}$ to the congruence $x^u \equiv y \pmod{p^2}$ is $O(1)$, where the implied constant depends only on u.*

Proof. For $p > u$, this follows immediately from Hensel's lemma and the fact that $\mathbb{Z}/p\mathbb{Z}$ is a field. When $p < |u|$, then $\#\mathbb{Z}/p^2\mathbb{Z}$ is bounded in terms of u, which concludes the proof. □

The bulk of the article is dedicated to proving Lemma 1.4 in the case that is not covered by [**5**, Theorem 4]. The technique is reminiscent of those in [**2**] and [**5**], but some complications appear. At some point we need to consider the resultant of two families of polynomials to guarantee that they do not have common roots very often. Finally, in §3, we give a proof of the main theorem. By classical methods of analytic number theory, we show how the result can be derived from Lemma 1.3 or 1.4, depending on the factorization of q.

§2. *Counting solutions to a congruence.* In this section we give a proof of Lemma 1.4 in the case where q is the square of a prime.

The proof is for a good part extremely similar to that of [**5**, Theorem 4] and we shall refer to that one at many steps.

By [**5**, equation (4.1)], we have that

$$S_{u,v}(M, N; q, a) \ll M^{1/4}\mathcal{N}_a(\mathcal{I})^{1/4} \tag{2.1}$$

for $\mathcal{I} = (0, N]$, where

$$\mathcal{N}_a(\mathcal{I}) = \frac{1}{q}\sum_{h=1}^{q}\left|\sum_{n\in\mathcal{I}}\sum_{\substack{m \pmod q \\ m^u \equiv an^v \pmod q}} e_q(hm)\right|^4 \tag{2.2}$$

and

$$\begin{aligned}\mathcal{N}_a(\mathcal{I}) = |\{(\boldsymbol{m}, \boldsymbol{n}),\ \boldsymbol{n} \in \mathcal{I}^4,\ \boldsymbol{m} \in (\mathbb{Z}/q\mathbb{Z})^4,\\ m_i^u \equiv an_i^v \pmod q \text{ for } 1 \leqslant i \leqslant 4\\ \text{and } m_1 + m_2 \equiv m_3 + m_4 \pmod q)\}|,\end{aligned}$$

https://doi.org/10.1112/S0025579317000043 Published online by Cambridge University Press

where here and throughout this section,

$$\boldsymbol{m} = (m_1, m_2, m_3, m_4) \quad \text{and} \quad \boldsymbol{n} = (n_1, n_2, n_3, n_4).$$

Notice that in order to quote directly the results from [5], we relaxed the condition $N/2 < n \leqslant N$ into $n \leqslant N$.

2.1. *A trivial bound.* Suppose that n_1, n_2 and n_3 are fixed. Then n_4 is determined modulo q and, by Lemma 1.5, we have at most $O(1)$ solutions for m_i modulo q for $1 \leqslant i \leqslant 4$. Thus, it follows that

$$\mathcal{N}_a(\mathcal{I}) \ll N^3\left(\frac{N}{q} + 1\right). \tag{2.3}$$

This estimate is not enough for our purposes and, as in [2] and [5], we need to introduce an auxiliary set of primes and benefit from averaging over this set.

2.2. *Introducing an auxiliary prime.* Fix a prime $p \nmid q$ such that $Q < p \leqslant 2Q$ with

$$Q < N \leqslant q, \tag{2.4}$$

where Q is a parameter to be chosen later.

We first separate the contribution to $N_a(\mathcal{I})$ of the quadruples (n_1, n_2, n_3, n_4) such that p divides one of the n_i. Analogously to (2.3), we have

$$\mathcal{N}_a(\mathcal{I}) \ll \frac{N^3}{Q}q^{\epsilon} + \frac{1}{q}\sum_{h=1}^{q}\Bigg|\sum_{\substack{n\in\mathcal{I}\\ p\mid n}}\sum_{\substack{m \pmod q\\ m^u\equiv an^v \pmod q}} e_q(hm)\Bigg|^4. \tag{2.5}$$

We shall now divide the remaining $n \in \mathcal{I}$ into residue classes modulo p. Since $p \nmid q$, every $n \in \mathcal{I}$ such that $p \nmid n$ is congruent to fq modulo p for some $1 \leqslant f \leqslant p-1$. Thus, by Hölder's inequality,

$$\Bigg|\sum_{\substack{n\in\mathcal{I}\\ p\nmid n}}\sum_{\substack{m \pmod q\\ m^u\equiv an^v \pmod q}} e_q(hm)\Bigg|^4 \ll Q^3\sum_{f=1}^{p-1}\Bigg|\sum_{\substack{n\in\mathcal{I}\\ n\equiv fq \pmod p}}\sum_{\substack{m \pmod q\\ m^u\equiv an^v \pmod q}} e_q(hm)\Bigg|^4.$$

Define the interval $\mathcal{I}(p, f) = (-fq/p, (N - fq)/p]$ and write $n = fq + ps$ with $s \in \mathcal{I}(p, f)$. Let

$$S(q; p, f) := \frac{1}{q}\sum_{h=1}^{q}\Bigg|\sum_{s\in\mathcal{I}(p,f)}\sum_{\substack{m \pmod q\\ m^u\equiv ap^v s^v \pmod q}} e_q(hm)\Bigg|^4.$$

Now let $\Gamma = (\mathbb{Z}/q\mathbb{Z})^{\times}$ and consider Γ/Γ^u, the quotient of Γ by the subgroup of uth powers in Γ. We know that

$$\Gamma/\Gamma^u \cong \{x \in \Gamma; x^u = 1\}.$$

https://doi.org/10.1112/S0025579317000043 Published online by Cambridge University Press

Thus, by Lemma 1.5,

$$|\Gamma/\Gamma^u| \ll 1. \tag{2.6}$$

Let $\{R_j, 1 \leqslant j \leqslant |\Gamma/\Gamma^u|\}$ be a complete set of coset representatives. Now suppose that $p = R_t g^u$ for some $1 \leqslant t \leqslant |\Gamma/\Gamma^u|$ and $g \in \Gamma$. We then have

$$S(q; p, f) = \frac{1}{q}\sum_{h=1}^{q}\Bigg|\sum_{s\in\mathcal{I}(p,f)}\sum_{\substack{m \pmod q\\ m^u\equiv aR_t^v g^{uv}s^v \pmod q}} e_q(hm)\Bigg|^4.$$

After a change of variables, we deduce that

$$S(q; p, f) = \frac{1}{q}\sum_{h=1}^{q}\Bigg|\sum_{s\in\mathcal{I}(p,f)}\sum_{\substack{m \pmod q\\ m^u\equiv aR_t^v s^v \pmod q}} e_q(hm)\Bigg|^4,$$

i.e.

$$S(q; p, f) = \mathcal{N}_b(\mathcal{I}(p, f)),$$

where $b = aR_t^u$. Assembling our last efforts, we obtain the inequality

$$\mathcal{N}_a(\mathcal{I}) \ll \frac{N^3}{Q}q^{\epsilon} + Q^3\sum_{f=1}^{p-1}\mathcal{N}_b(\mathcal{I}(p, f)).$$

The importance of the above formula is that it only depends on the class of p in Γ/Γ^u. This will be especially important when we average over p.

2.3. *Averaging over the set of primes.* At this point we need to separate the set of quadruples $\boldsymbol{n} \in \mathbb{Z}^4$ into "good" and "bad". The good set is chosen so that we can benefit from averaging and the bad set is small enough so that averaging is not necessary.

After splitting the sum according to whether $\boldsymbol{n}$ is good or bad, we need to treat these sums and then introduce the set of primes over which we average. At this point we make crucial use of the finiteness of $|\Gamma/\Gamma^u|$ deduced in the previous subsection (see (2.6)). The argument is identical to that in [**5**, §4.3], so we shall content ourselves to quote the results from there.

Before we continue, we need to introduce some notation. Suppose that B and G are two distinct sets such that $B \cup G = \mathbb{Z}^4$. Let

$$\begin{aligned}\mathcal{N}_b^B(t) = |\{(\boldsymbol{m}, \boldsymbol{n}); \boldsymbol{m}(\in \mathbb{Z}/q\mathbb{Z})^4, \boldsymbol{n} \in B, \boldsymbol{n} \in (-t, NQ^{-1} - t]^4,\\ m_i^u \equiv bn_i^v \pmod q \text{ for } 1 \leqslant i \leqslant 4\\ \text{and } m_1 + m_2 \equiv m_3 + m_4 \pmod q)\}|\end{aligned} \tag{2.7}$$

and let

$$K_b = \sup_{t\in\mathbb{R}} N_b^B(t).$$

https://doi.org/10.1112/S0025579317000043 Published online by Cambridge University Press

Finally, we let

$$L_b = |\{(\boldsymbol{m}, \boldsymbol{n}, j);\ \boldsymbol{m} \in (\mathbb{Z}/q\mathbb{Z})^4,\ \boldsymbol{n} \in (0, NQ^{-1}]^4,\ 1 \leqslant j \leqslant q,\\ \boldsymbol{n} - j \in G,\ m_i^u \equiv b(n_i - j)^v \pmod q \text{ for } 1 \leqslant i \leqslant 4\\ \text{and } m_1 + m_2 \equiv m_3 + m_4 \pmod q)\}|,$$

where

$$\boldsymbol{n} - j := (n_1 - j, \dots, n_4 - j).$$

We are now ready to quote the results from [5]. With the notation as above, it follows from [5, equation (4.3)] that we have the inequality

$$\mathcal{N}_a(\mathcal{I}) \ll N^3 Q^{-1} q^{\epsilon} + Q^4 K_b + Q^3 N^{-1} (\log Q) L_b \tag{2.8}$$

provided that

$$8NQ \leqslant q. \tag{2.9}$$

2.4. *The good and the bad sets.* We write again $q = p_0^2$ and we let the bad set B consist of the quadruples $\boldsymbol{n} \in \mathbb{Z}^4$ for which there exists $(x_1, x_2, x_3, x_4) \in (\mathbb{Z}/p_0\mathbb{Z})^4$ such that

$$\begin{cases} x_i^u \equiv b n_i^v \pmod{p_0} \quad \text{for } 1 \leqslant i \leqslant 4, \\ x_1 + x_2 \equiv x_3 + x_4 \pmod{p_0}, \\ \dfrac{x_1}{n_1} + \dfrac{x_2}{n_2} \equiv \dfrac{x_3}{n_3} + \dfrac{x_4}{n_4} \pmod{p_0}. \end{cases}$$

And, naturally, $G = \mathbb{Z}^4 \backslash B$. With B and G as above, we must now estimate K_b and L_b.

2.5. *Estimating L_b.* We let

$$L_b = \sum_{\boldsymbol{n}} L_b(\boldsymbol{n}, q),$$

where $L_b(\boldsymbol{n}, q)$ is the contribution to L_b for a fixed quadruple $\boldsymbol{n}$.

It follows from [5, top of p. 594] that unless (n_3, n_4) is a permutation of (n_1, n_2), we have the inequality

$$L_b(\boldsymbol{n}, p_0) \ll p_0^{\epsilon}.$$

We shall deduce that with the above choice for G, we have the same inequality for $L_b(\boldsymbol{n}, q)$.

Suppose that $(x_1, x_2, x_3, x_4, y) \in (\mathbb{Z}/p_0\mathbb{Z})^5$ is a solution to the system of congruences

$$\begin{cases} x_i^u \equiv b(n_i - y)^v \pmod{p_0} \quad \text{for } 1 \leqslant i \leqslant 4, \\ x_1 + x_2 \equiv x_3 + x_4 \pmod{p_0}. \end{cases} \tag{2.10}$$

https://doi.org/10.1112/S0025579317000043 Published online by Cambridge University Press

We shall prove that this solution cannot be lifted to $(\mathbb{Z}/q\mathbb{Z})^5$ in too many ways. Suppose that (m_1, m_2, m_3, m_4, j) and $(m_1', m_2', m_3', m_4', j')$ in $(\mathbb{Z}/q\mathbb{Z})^5$ are two different solutions to the system of congruences

$$\begin{cases} m_i^u \equiv b(n_i - j)^v \pmod q \quad \text{for } 1 \leqslant i \leqslant 4, \\ m_1 + m_2 \equiv m_3 + m_4 \pmod q, \\ m_i \equiv x_i \pmod{p_0} \quad \text{for } 1 \leqslant i \leqslant 4, \\ j \equiv y \pmod{p_0}. \end{cases}$$

Let ℓ be such that $j' = j + \ell p_0$. We have that

$$\begin{aligned} m_i' - m_i &\equiv \frac{(m_i')^u - (m_i)^u}{\sum_{s=0}^{u-1}(m_i')^s m_i^{u-1-s}} \pmod q \\ &\equiv b\frac{(n_i - j - \ell p_0)^v - (n_i - j)^v}{\sum_{s=0}^{u-1}(m_i')^s m_i^{u-1-s}} \pmod q \\ &\equiv \frac{bv\ell p_0 (n_i - j)^{v-1}}{\sum_{s=0}^{u-1}(m_i')^s m_i^{u-1-s}} \pmod q. \end{aligned}$$

Now, since $\sum_{s=0}^{u-1}(m_i')^s m_i^{u-1-s} \equiv u x_i^{u-1} \pmod{p_0}$, $p_0 > |u| + |v|$ and

$$m_1 + m_2 - m_3 - m_4 \equiv m_1' + m_2' - m_3' - m_4' \equiv 0 \pmod q,$$

we deduce that either $\ell \equiv 0 \pmod{p_0}$ or

$$\frac{(n_1 - j)^{v-1}}{x_1^{u-1}} + \frac{(n_2 - j)^{v-1}}{x_2^{u-1}} \equiv \frac{(n_3 - j)^{v-1}}{x_3^{u-1}} + \frac{(n_4 - j)^{v-1}}{x_4^{u-1}} \pmod{p_0}.$$

We recall that $x_i^u \equiv b(n_i - j)^v \pmod{p_0}$. Thus, we must have

$$\frac{x_1}{(n_1 - j)} + \frac{x_2}{(n_2 - j)} \equiv \frac{x_3}{(n_3 - j)} + \frac{x_4}{(n_4 - j)} \pmod{p_0}.$$

But the above congruence is impossible in view of (2.10) and the fact that $\boldsymbol{n} - j$ is a good quadruple. We then conclude that we must have $\ell = 0$ and, hence, by Hensel's lemma, $m_i = m_i'$. We have just proved that

$$L_b(\boldsymbol{n}, q) = L_b(\boldsymbol{n}, p_0) \ll q^{\epsilon}.$$

https://doi.org/10.1112/S0025579317000043 Published online by Cambridge University Press

Summing over $\boldsymbol{n}$, we deduce that

$$L_b \ll (NQ^{-1})^4 q^{\epsilon}. \tag{2.11}$$

2.6. *Estimating K_b.* We shall estimate K_b by means of the following lemma.

LEMMA 2.1. *Let p be a prime number and let $\mathbb{F}_p$ be a field with p elements. Let $\alpha, \beta, \gamma \in (\mathbb{F}_p)^{\times}$. We also let k and ℓ be two distinct non-zero integers. Then the number of solutions in (X_1, X_2, Y_1, Y_2) to the system of equations*

$$\begin{cases} X_1 + X_2 = \alpha, \\ Y_1 + Y_2 = \beta, \\ X_i^k = \gamma Y_i^{\ell} \text{ for } i = 1, 2 \end{cases} \tag{2.12}$$

is $O(1)$, where the implied constant depends at most on k and ℓ.

Proof. We start by noticing that we may assume that $p > \max(|k|, |\ell|)$, since, otherwise, even without considering the equations (2.12), the number of quadruples (X_1, X_2, Y_1, Y_2) is bounded in terms of k and ℓ.

We notice that the variables X_2 and Y_2 are completely determined by X_1 and Y_1. Thus, (2.12) is equivalent to the system

$$\begin{cases} X^k = \gamma Y^{\ell}, \\ (\alpha - X)^k = \gamma(\beta - Y)^{\ell}. \end{cases} \tag{2.13}$$

Notice that there is no harm in supposing that $k > 0$, since, otherwise, it suffices to replace (k, ℓ, γ) by $(-k, -\ell, \gamma^{-1})$.

Now there are two cases to consider. We have either $\ell > 0$ or $\ell < 0$. For the rest of this proof, we let $\overline{\mathbb{F}_p}$ denote an algebraic closure of $\mathbb{F}_p$.

First case: $\ell > 0$. We also suppose that $k > \ell$. The other case is analogous with only the roles of α and β interchanged.

We let $P_Y(X) = X^k - \gamma Y^{\ell}$ and $Q_Y(X) = (\alpha - X)^k - \gamma(\beta - Y)^{\ell}$. For every $Y \in \mathbb{F}_p$, these two polynomials have a common root if and only if their resultant $R(Y) = \mathrm{Res}(P_Y, Q_Y)$ vanishes.

Now, since the coefficients of P_Y and Q_Y are polynomials in Y, it follows that $R(Y)$ is itself a polynomial in Y. If we can prove that $R(Y)$ is not identically zero, then we will deduce that there are at most $O(1)$ solutions to $R(Y) = 0$ and, since $X^k = \gamma Y^{\ell}$, we will be done.

To prove that $R \not\equiv 0$, we consider the polynomial $\tilde{R}(Y) := R(Y^k)$. The main reason is that we have the factorization

$$P_{Y^k}(X) = \prod_{j=1}^{k} (X - \eta_j Y^{\ell}),$$

where the $\eta_j \in \overline{\mathbb{F}_p}$ are such that $X^k - \gamma = \prod_{j=1}^{k}(X - \eta_j)$. In particular, $\eta_j^k = \gamma$.

https://doi.org/10.1112/S0025579317000043 Published online by Cambridge University Press

It follows from the definition of resultant that

$$\begin{aligned} R(Y^k) &= \prod_{j=1}^{k} Q_{Y^k}(\eta_j Y^\ell) \\ &= \prod_{j=1}^{k} ((\alpha - \eta_j Y^\ell)^k - \gamma(\beta - Y^k)^\ell) \\ &= \prod_{j=1}^{k} ((-1)^k \gamma Y^{k\ell} + (-1)^{\ell-1} \gamma Y^{k\ell} + (-1)^\ell \beta\gamma\ell Y^{k\ell-\ell} + \cdots), \end{aligned}$$

where the omitted terms have degree $< k\ell - \ell$. There are two possible cases. If k and ℓ have opposite parities, then

$$R(Y^k) = \pm\gamma^k Y^{k^2\ell} + \cdots$$

and thus $R \not\equiv 0$. If, however k and ℓ have the same parity, then

$$R(Y^k) = \pm(\beta\gamma\ell)^k Y^{k^2\ell - k\ell} + \cdots$$

and, again, we have $R \not\equiv 0$.

Second case: $\ell < 0$. This case is actually simpler. Consider the polynomials $P_Y(X) = Y^{|\ell|}X^k - \gamma$, $Q_Y(X) = (\beta - Y)^{|\ell|}(\alpha - X)^k$. Notice that we may assume that Y is not equal to 0 or β, since $\ell < 0$. Analogously to the previous case, we let $R(Y) = \mathrm{Res}(P_Y, Q_Y)$, which is a polynomial in Y. Let η_j, $1 \leqslant j \leqslant k$, be as before. It follows that

$$P_{Y^k}(X) = Y^{k|\ell|} \prod_{j=1}^{k} (X - \eta_j Y^{-|\ell|}).$$

Thus,

$$\begin{aligned} R(Y^k) &= Y^{k^2|\ell|} \prod_{j=1}^{k} Q_{Y^k}(\eta_j Y^{-|\ell|}) \\ &= Y^{k^2|\ell|} \prod_{j=1}^{k} ((\beta - Y^k)^{|\ell|}(\alpha - \eta_j Y^{-|\ell|})^k - \gamma) \\ &= \prod_{j=1}^{k} ((\beta - Y^k)^{|\ell|}(\alpha Y^{|\ell|} - \eta_j)^k - \gamma). \end{aligned}$$

It readily follows that $R(Y^k) = \pm\alpha^{k^2} Y^{2k^2\ell} + \cdots$. Hence, $R \not\equiv 0$. This completes the proof of the lemma. □

https://doi.org/10.1112/S0025579317000043 Published online by Cambridge University Press

With our definition of bad quadruples, $\mathcal{N}_b^B$ is bounded by the number of solutions in $(\boldsymbol{m}, \boldsymbol{n})$ such that $m_i \in (\mathbb{Z}/p_0^2\mathbb{Z})^\times$, $n_i \in (-t, NQ^{-1} - t]$ and

$$\begin{cases} x_i^u \equiv bn_i^v \pmod q, \ 1 \leqslant i \leqslant 4, \\ x_1 + x_2 \equiv x_3 + x_4 \pmod{p_0}, \\ \dfrac{x_1}{n_1} + \dfrac{x_2}{n_2} \equiv \dfrac{x_3}{n_3} + \dfrac{x_4}{n_4} \pmod{p_0}. \end{cases}$$

Suppose that we fix n_3, n_4; then there are at most $O(1)$ possibilities for m_3 and m_4. We let $m_3 + m_4 = \alpha$, $m_3/n_3 + m_4/n_4 = \beta$. If we let, for $i = 1, 2$, $y_i = x_i/n_i$, then (x_1, x_2, y_1, y_2) is a solution to the system (2.12) with $k = v - u$, $\ell = v$ and $\gamma = 1/b$.

It follows from Lemma 2.1 that if $\alpha\beta \not\equiv 0 \pmod{p_0}$, we have at most $O(1)$ solutions for x_i and $y_i \pmod{p_0}$. This determines m_1, m_2, n_1 and n_2. Hensel's lemma now says that this also determines the m_i completely.

Summarizing, we see that the number of solutions in this case is at most

$$(NQ^{-1})^2(NQ^{-1}p_0^{-1} + 1)^2. \tag{2.14}$$

We shall now estimate the contribution of the terms where $m_3 + m_4 \equiv 0 \pmod{p_0}$ or $m_3/n_3 + m_4/n_4 \equiv 0 \pmod{p_0}$. We consider only the first case, since the other one is analogous.

Notice that $m_3 + m_4 = 0$ implies that $n_3^v \equiv \pm n_4^v \pmod{p_0}$, so that each value of n_3 determines at most $O(1)$ solutions for $n_4 \pmod{p_0}$. The same is true for n_1 and n_2. And, finally, each of these quadruples determines at most $O(1)$ solutions for $\boldsymbol{m}$. Hence, the total contribution of the terms where $\alpha = 0$ or $\beta = 0$ is at most (2.14) as well. Thus, we have proved that

$$K_b \ll (NQ^{-1})^2(NQ^{-1}p_0^{-1} + 1)^2. \tag{2.15}$$

2.7. *End of proof of Lemma 1.4.* We now combine our various estimates and give a bound for $\mathcal{N}(\mathcal{I})$.

Gathering (2.8), (2.11) and (2.15), we prove that

$$\mathcal{N}(\mathcal{I}) \ll (N^3Q^{-1} + N^4q^{-1} + N^2Q^2)q^\epsilon$$

provided that N and Q satisfy (2.4) and (2.9). By choosing $Q = \frac{1}{8}N^{1/3}$, we see that

$$\mathcal{N}(\mathcal{I}) \ll N^{8/3}q^\epsilon \tag{2.16}$$

provided that $N \leqslant q^{3/4}$. Lemma 1.4 now follows from (2.1) and (2.16).

§3. *Proof of Theorem 1.1.* In the present section we give a proof of Theorem 1.1.

https://doi.org/10.1112/S0025579317000043 Published online by Cambridge University Press

3.1. *Initial steps.* Let q be a positive integer, let a be coprime with q and $X \geqslant q$. We consider $E = E(X, q, a)$ given by

$$E := \sum_{\substack{n \leqslant X \\ n \equiv a \pmod q}} \mu^2(n) - \frac{1}{\varphi(q)} \sum_{\substack{n \leqslant X \\ (n,q)=1}} \mu^2(n).$$

Our goal is to prove that we have the inequality $E \ll X^{1-\delta}/q$ uniformly for $q \leqslant X^{25/36-\epsilon}$.

If $q \leqslant X^{1/2}$, then this already follows from (1.1). Therefore, we may suppose that

$$q \geqslant X^{1/2}.$$

We recall the classical identity

$$\mu^2(n) = \sum_{\substack{n_1, n_2 \geqslant 1 \\ n_1 n_2^2 = n}} \sum \mu(n_2). \tag{3.1}$$

This gives

$$E = \sum_{\substack{n \leqslant X^{1/2} \\ (n,q)=1}} \mu(n) \Delta(X/n^2, q, a\bar{n}^2),$$

where, for every $x \geqslant 1$, q an integer and $a \in \mathbb{Z}/q\mathbb{Z}$,

$$\Delta(x, q, a) := \sum_{\substack{m \leqslant x \\ m \equiv a \pmod q}} 1 - \frac{1}{\varphi(q)} \sum_{\substack{m \leqslant x \\ (m,q)=1}} 1.$$

It is clear that for any x, q, a, we have

$$\Delta(x, q, a) \ll d(q).$$

Let N_0 be a parameter to be chosen optimally later and such that $1 \leqslant N_0 \leqslant X^{1/2}$. The previous inequality shows us that

$$E = \sum_{\substack{N_0 < n \leqslant X^{1/2} \\ (n,q)=1}} \mu(n) \Delta(X/n^2, q, a\bar{n}^2) + O(N_0 q^{\epsilon}). \tag{3.2}$$

Notice that

$$\frac{1}{\varphi(q)} \sum_{\substack{N_0 < n \leqslant X^{1/2} \\ (n,q)=1}} \mu(n) \sum_{\substack{m \leqslant X/n^2 \\ (m,q)=1}} 1 \ll \frac{X^{1+\epsilon}}{N_0 q}.$$

This and (3.2) combined give

$$|E| \leqslant \sum_{\substack{N_0 < n \leqslant X^{1/2} \\ (n,q)=1}} \sum_{\substack{m \leqslant X/n^2 \\ m \equiv a\bar{n}^2 \pmod q}} 1 + O\left(X^{\epsilon} \left(N_0 + \frac{X^{1+\epsilon}}{N_0 q} \right) \right). \tag{3.3}$$

https://doi.org/10.1112/S0025579317000043 Published online by Cambridge University Press

3.2. *Division into dyadic boxes.* We now proceed by means of a dyadic decomposition. If we put

$$S(M, N, q, a) = \sum_{\substack{m\sim M,\, n\sim N \\ mn^2\equiv a \pmod q}}\sum 1, \tag{3.4}$$

we deduce from (3.3) the upper bound

$$E \ll (\log X)^2 \cdot \sup_{M,N} S(M, N, q, a) + X^\epsilon\left(N_0 + \frac{X}{N_0 q}\right),$$

where the supremum is taken over all M and N such that

$$M, N \geqslant 1, \qquad N_0 \leqslant N \leqslant 2X^{1/2}, \qquad MN^2 \leqslant 8X. \tag{3.5}$$

Let $M_0 \geqslant 1$ be a parameter to be chosen optimally later. Suppose that $M \leqslant M_0$ and that M, N satisfy the conditions (3.5). Then, by the crude estimate

$$\sum_{\substack{n\sim N \\ n\equiv\alpha \pmod q}} 1 \ll \frac{N}{q} + 1,$$

we see that

$$\begin{aligned} S(M, N, q, a) &\ll Mq^\epsilon\left(\frac{N}{q} + 1\right) \\ &\ll X^\epsilon\left(\frac{X}{N_0 q} + M_0\right). \end{aligned}$$

Thus,

$$E \ll (\log X)^2 \sup_{M,N} S(M, N, q, a) + X^\epsilon\left(M_0 + N_0 + \frac{X}{N_0 q}\right), \tag{3.6}$$

where now the supremum is taken over all M and N satisfying

$$M \geqslant M_0, \qquad N \geqslant N_0, \qquad MN^2 \leqslant 8X. \tag{3.7}$$

3.3. *Conclusion.* We notice that

$$S(M, N, q, a) = S_{1,-2}(M, N, q, a). \tag{3.8}$$

Before we continue, we make the trivial remark that if q_0 divides q, then

$$S(M, N, q, a) \leqslant S(M, N, q_0, a). \tag{3.9}$$

Our final estimation will in fact depend on the factorization of q. The next lemma tells us that we can always find a divisor of q satisfying certain conditions about its size.

https://doi.org/10.1112/S0025579317000043 Published online by Cambridge University Press

LEMMA 3.1. *Let $q \geqslant 1$ be an integer. Then at least one of the following holds.*

(i) *There exists $q_0 \mid q$ such that $q^{14/25} \leqslant q_0 \leqslant q^{22/25}$.*

(ii) *There exists $q_0 \mid q$ such that $q_0 \geqslant q^{22/25}$ and q_0 is either squarefree or the square of a prime number.*

Proof. Let $q = \prod_p p^f$ denote the prime factorization of q and let

$$q_1 = \prod_{p \leqslant q^{3/25}} p^f.$$

Suppose that $q_1 \geqslant q^{3/25}$. Then it follows that there exists $q_2 \mid q_1$ such that $q^{3/25} < q_2 < q^{6/25}$. By taking $q_0 = q/q_2$, we see that (i) holds in this case.

Now suppose that $q_1 < q^{3/25}$ and let $q_3 = q/q_1$. We have $q_3 > q^{22/25}$. If there exists a prime number p such that $p \mid q_3$ and $q^{3/25} < p < q^{11/25}$ or $q^{14/25} < p < q^{22/25}$, then (i) follows in this case as well.

Finally, we are left with the case where q has a divisor q_3 such that $q_3 \geqslant q^{22/25}$ and every divisor of q_3 satisfies $q^{11/25} < p < q^{14/25}$. We deduce that q_3 must be a product of exactly two primes, not necessarily distinct. It readily follows that (ii) holds in this case. □

We shall now derive upper bounds for $S(M, N; q, a)$ in both cases described by Lemma 3.1.

First case: suppose that there exists $q_0 \mid q$ such that $q^{14/25} < q_0 < q^{22/25}$. We make the following choices:

$$M_0 = \max(X/q_0^2, 1), \qquad N_0 = (X/q_0)^{1/2}.$$

It then follows that for every M, N satisfying (3.7), we have

$$M, N \ll q_0.$$

Hence, by (3.9) and Lemma 1.3,

$$\begin{aligned} S(M, N; q, a) &\ll X^{\epsilon}(MNq_0^{-1} + q_0^{1/2}) \\ &\ll X^{\epsilon}(X^{1/2}q_0^{-1/2} + q_0^{1/2}) \\ &\ll X^{\epsilon}(X^{1/2}q^{-7/25} + q^{11/25}). \end{aligned} \tag{3.10}$$

Hence, by (3.6), we have

$$|E| \leqslant X^{\epsilon}(Xq^{-28/25} + X^{1/2}q^{-7/25} + q^{11/25}). \tag{3.11}$$

Second case: suppose that there exists $q_0 \mid q$ such that q_0 is either squarefree or the square of a prime and $q_0 > q^{22/25}$. We make the choices

$$M_0 = \max(Xq_0^{-3/2}, 1), \qquad N_0 = X^{1/2}q_0^{-3/8}. \tag{3.12}$$

https://doi.org/10.1112/S0025579317000043 Published online by Cambridge University Press

It then follows that for every M, N satisfying (3.7), we have

$$M, N \ll q_0^{3/4}.$$

Lemma 1.4, (3.8) and (1.9) now give the upper bound

$$S(M, N, q, a) \ll q^{\epsilon} \min(M^{2/3}N^{1/4}, M^{1/4}N^{2/3}) \tag{3.13}$$

for every M, N satisfying (3.7). It is not hard to see that for every $0 < \alpha < 1$, (3.13) implies the inequality

$$S(M, N, q, a) \ll q^{\epsilon}(M^{2/3}N^{1/4})^{\alpha}(M^{1/4}N^{2/3})^{1-\alpha}. \tag{3.14}$$

Taking $\alpha = 2/15$, we get

$$S(M, N, q, a) \ll q^{\epsilon}(MN^2)^{11/36} \leqslant X^{11/36+\epsilon}.$$

Now, by (3.6) and (3.12), we see that

$$E \ll X^{11/36+\epsilon} + Xq^{-33/25} + X^{1/2}q^{-33/100}. \tag{3.15}$$

Combining (3.11) and (3.15), we obtain the bound

$$E \ll X^{11/36+\epsilon} + Xq^{-28/25} + X^{1/2}q^{-7/25}.$$

It is now straightforward to verify that for every $\epsilon > 0$, there exists $\delta = \delta(\epsilon) > 0$ such that whenever $q \leqslant X^{25/36-\epsilon}$, we have the inequality

$$E \ll \frac{X^{1-\delta}}{q}.$$

This concludes the proof of Theorem 1.1.

Acknowledgements. I am very thankful to Étienne Fouvry and Philippe Michel for many useful discussions and helpful remarks. I also would like to express my gratitude to the referee for his careful reading of the manuscript.

References

1. P. Erdős, Über die kleinste quadratfreie Zahl einer arithmetischen Reihe. *Monatsh. Math.* **64** (1960), 314–316 (in German).
2. D. R. Heath-Brown, The least square-free number in an arithmetic progression. *J. Reine Angew. Math.* **332** (1982), 204–220.
3. C. Hooley, A note on square-free numbers in arithmetic progressions. *Bull. Lond. Math. Soc.* **7** (1975), 133–138.
4. R. M. Nunes, Squarefree numbers in large arithmetic progressions. *Preprint*, 2016, arXiv:1602.00311.

https://doi.org/10.1112/S0025579317000043 Published online by Cambridge University Press

5. L. B. Pierce, The 3-part of class numbers of quadratic fields. *J. Lond. Math. Soc.* (2) **71**(3) (2005), 579–598.
6. K. Prachar, Über die kleinste quadratfreie Zahl einer arithmetischen Reihe. *Monatsh. Math.* **62** (1958), 173–176 (in German).

R. M. Nunes,
EPFL SB MATHGEOM TAN,
Station 8,
CH-1015 Lausanne,
Switzerland
E-mail: ramon.moreiranunes@epfl.ch

https://doi.org/10.1112/S0025579317000043 Published online by Cambridge University Press