Michigan Math. J. 59 (2010), 313–328

On the Divisibility of Fermat Quotients

Jean Bourgain, Kevin Ford,
Sergei V. Konyagin, & Igor E. Shparlinski

1. Introduction

For a prime p and an integer a the *Fermat quotient* is defined as

$$q_p(a) = \frac{a^{p-1} - 1}{p}.$$

It is well known that divisibility of Fermat quotients $q_p(a)$ by p has numerous applications, which include Fermat's last theorem and squarefreeness testing; see [6; 7; 8; 16].

In particular, the smallest value ℓ_p of a for which $q_p(a) \not\equiv 0 \pmod p$ plays a prominent role in these applications. In this direction, Lenstra [16, Thm. 3] has shown that

$$\ell_p \le \begin{cases} 4(\log p)^2 & \text{if } p \ge 3, \\ (4e^{-2} + o(1))(\log p)^2 & \text{if } p \to \infty; \end{cases} \tag{1}$$

see also [7]. Granville [9, Thm. 5] has shown that in fact

$$\ell_p \le (\log p)^2 \tag{2}$$

for $p \ge 5$.

A very different proof of a slightly weaker bound $\ell_p \le (4 + o(1))(\log p)^2$ has been obtained by Ihara [12] as a by-product of the estimate

$$\sum_{\substack{\ell^k < p \\ \ell \in \mathcal{W}(p)}} \frac{\log \ell}{\ell^k} \le 2 \log\log p + 2 + o(1) \tag{3}$$

as $p \to \infty$, where the summation is taken over all prime powers up to p of primes ℓ from the set

$$\mathcal{W}(p) = \{\ell \text{ prime} : \ell < p,\ q_p(\ell) \equiv 0 \pmod p\}.$$

However, the proof of (3) given in [12] is conditional on the extended Riemann hypothesis.

It has been conjectured by Granville [8, Conj. 10] that

$$\ell_p = o((\log p)^{1/4}). \tag{4}$$

Received December 22, 2008. Revision received August 14, 2009.

It is quite reasonable to expect a much stronger bound on ℓ_p. For example, Lenstra [16] conjectures that $\ell_p \le 3$; this has been supported by extensive computation (see [5; 14]). The motivation for the conjecture (4) comes from the fact that this has some interesting applications to Fermat's last theorem [8, Cor. 1]. Although this motivation relating ℓ_p to Fermat's last theorem does not exist anymore, improving the bounds (1) and (2) is still of interest and may have some other applications.

THEOREM 1. *We have*

$$\ell_p \le (\log p)^{463/252+o(1)}$$

as $p \to \infty$.

Following the arguments of [16], we derive the following improvement of [16, Thm. 2].

COROLLARY 2. *For every* $\varepsilon > 0$ *and a sufficiently large integer* n, *if* $a^{n-1} \equiv 1 \pmod n$ *for every positive integer* $a \le (\log n)^{463/252+\varepsilon}$ *then* n *is squarefree.*

The proof of Theorem 1 is based on the original idea of Lenstra [16], which relates ℓ_p to the distribution of smooth numbers, which we also supplement by some recent results on the distribution of elements of multiplicative subgroups of residue rings of Bourgain, Konyagin, and Shparlinski [3] combined with a bound of Heath-Brown and Konyagin [10] for Heilbronn exponential sums. Also, using these results we can prove the following.

THEOREM 3. *For every* $\varepsilon > 0$, *there is* $\delta > 0$ *such that for all but one prime* $Q^{1-\delta} < p \le Q$, *we have* $\ell_p \le (\log p)^{59/35+\varepsilon}$.

The proof of the next result is based on a large sieve inequality with square moduli that is due to Baier and Zhao [1].

THEOREM 4. *For every* $\varepsilon > 0$, *there is* $\delta > 0$ *such that for all but* $O(Q^{1-\delta})$ *primes* $p \le Q$, *we have* $\ell_p \le (\log p)^{5/3+\varepsilon}$.

We note that

$$\frac{463}{252} = 1.8373\ldots, \quad \frac{59}{35} = 1.6857\ldots, \quad \frac{5}{3} = 1.6666\ldots.$$

Throughout the paper, the implied constants in the symbols "O" and "$\ll$" may occasionally depend on the positive parameters ε and δ, and are absolute otherwise. We recall that the notations $U = O(V)$ and $U \ll V$ are both equivalent to the assertion that the inequality $|U| \le cV$ holds for some constant $c > 0$.

2. Smooth Numbers

For any integer n we write $P(n)$ for the largest prime factor of an integer n with the convention that $P(0) = P(\pm 1) = 1$.

For $x \ge y \ge 2$ we define $\mathcal{S}(x, y)$ as the set y-smooth numbers up to x, that is

$$\mathcal{S}(x, y) = \{n \le x : P(n) \le y\}$$

and put

$$\Psi(x, y) = \#\mathcal{S}(x, y).$$

We make use of the following explicit estimate, which is due to Konyagin and Pomerance [15, Thm. 2.1] (see also [11] for a variety of other results).

LEMMA 5. *If $x \ge 4$ and $x \ge y \ge 2$, then*

$$\Psi(x, y) > x^{1-\log\log x/\log y}.$$

3. Heilbronn Sums

For an integer $m \ge 1$ and a complex z, we put

$$\mathbf{e}_m(z) = \exp(2\pi i z/m).$$

Let $\mathbb{Z}_n$ be the ring of integers modulo an $n \ge 1$ and let $\mathbb{Z}_n^*$ be the group of units of $\mathbb{Z}_n$.

Now, for a prime p and an integer λ, we define the *Heilbronn sum*

$$H_p(\lambda) = \sum_{b=1}^{p} \mathbf{e}_{p^2}(\lambda b^p).$$

For $x \in \mathbb{Z}_p$ denote

$$f(x) = x + \frac{x^2}{2} + \cdots + \frac{x^{p-1}}{p-1} \in \mathbb{Z}_p. \tag{5}$$

Also, define for $u \in \mathbb{Z}_p$

$$\mathcal{F}(u) = \{x \in \mathbb{Z}_p : f(x) = u\}. \tag{6}$$

We now recall the following two results due to Heath-Brown and Konyagin that are [10, Thm. 2] and [10, Lemma 7], respectively.

LEMMA 6. *Uniformly over all $s \not\equiv 0 \bmod p$, we have*

$$\sum_{r=1}^{p} |H_p(s + rp)|^4 \ll p^{7/2}.$$

LEMMA 7. *Let $\mathcal{U}$ be a subset of $\mathbb{Z}_p$ and $T = \#\mathcal{U}$. Then*

$$\sum_{u\in\mathcal{U}} \#\mathcal{F}(u) \ll (pT)^{2/3}.$$

Since $H_p(rp) = 0$ if $r \not\equiv 0 \bmod p$ and $H_p(rp) = p$ if $r \equiv 0 \bmod p$, we immediately derive from Lemma 6 that

$$\sum_{u=1}^{p^2} |H_p(u)|^4 \ll p^{9/2}. \tag{7}$$

4. Distribution of Elements of Multiplicative Subgroups in Residue Rings

Given a multiplicative subgroup $\mathcal{G}$ of $\mathbb{Z}_n^*$, we consider its coset in $\mathbb{Z}_n^*$ (or multiplicative translate) $\mathcal{A} = \lambda\mathcal{G}$, where $\lambda \in \mathbb{Z}_n^*$. For an integer K and a positive integer k, we denote

$$J(n, \mathcal{A}, k, K) = \#(\{K+1, \dots, K+k\} \cap \mathcal{A}).$$

We need the following estimate from [3].

LEMMA 8. *Let $\mathcal{A}$ be a coset of a multiplicative subgroup $\mathcal{G}$ of $\mathbb{Z}_n^*$ of order t. Then, for any fixed $\varepsilon > 0$, we have*

$$J(n, \mathcal{A}, k, K) \ll \frac{kt}{n} + \frac{k}{tn} \sum_{w \in \mathbb{Z}_n} M_n(w; Z, \mathcal{G}) \left| \sum_{u \in \mathcal{A}} \mathbf{e}_n(uw) \right|,$$

where

$$Z = \min\{n^{1+\varepsilon} k^{-1}, n/2\}$$

and $M_n(w; Z, \mathcal{G})$ is the number of solutions to the congruence

$$w \equiv zu \pmod n, \quad 1 \le |z| \le Z, \ u \in \mathcal{G}.$$

Let $N(n, \mathcal{G}, Z)$ be the number of solutions of the congruence

$$ux \equiv y \pmod n, \quad \text{where } 0 < |x|, |y| \le Z, \text{ and } u \in \mathcal{G}.$$

We use Lemma 8 in a combination with yet another result from [3], which gives an upper bound on $N(n, \mathcal{G}, Z)$. We note that the proof given in [3] works only for $Z \ge n^{1/2}$, which is always satisfied in this paper; however it is shown in [4] that the result holds without this condition too, exactly as it is formulated in [3].

LEMMA 9. *Let $\nu \ge 1$ be a fixed integer and let $n \to \infty$. Assume $\#\mathcal{G} = t \gg \sqrt{n}$. Then for any positive number Z we have*

$$N(n, \mathcal{G}, Z) \le Z t^{(2\nu+1)/(2\nu(\nu+1))} n^{-1/(2(\nu+1))+o(1)} + Z^2 t^{1/\nu} n^{-1/\nu+o(1)}.$$

5. Large Sieve for Square Moduli

We make use of the following result of Baier and Zhao [1, Thm. 1].

LEMMA 10. *Let $\alpha_1, \dots, \alpha_N$ be an arbitrary sequence of complex numbers and let*

$$Y = \sum_{n=1}^{N} |\alpha_n|^2 \quad \text{and} \quad S(u) = \sum_{n=1}^{N} \alpha_n \exp(2\pi i u n).$$

Then, for any fixed $\varepsilon > 0$ and arbitrary $Q \ge 1$, we have

$$\sum_{1 \le q \le Q} \sum_{\substack{a=1 \\ \gcd(a,q)=1}}^{q^2} \left| S\left(\frac{a}{q^2}\right) \right|^2 \ll (QN)^{\varepsilon} (Q^3 + N + \min\{NQ^{1/2}, N^{1/2}Q^2\}) Y.$$

6. Proof of Theorem 1

For a positive integer $k < p^2$, let $N_p(k)$ denote the number of elements $v \in [1, k]$ of the subgroup $\mathcal{G} \subseteq \mathbb{Z}_{p^2}^*$ of order $p-1$, consisting of nonzero pth powers in $\mathbb{Z}_{p^2}$. We fix some $\varepsilon > 0$.

To get an upper bound on $N_p(k)$ we use Lemma 8, which we apply with $n = p^2$, $\mathcal{A} = \mathcal{G}$, $t = p-1$, and $K = 0$. For every integer a with $a^{p-1} \equiv 1 \pmod{p^2}$ there is a unique integer b with $1 \le b \le p-1$ such that $a \equiv b^p \pmod{p^2}$. Thus the corresponding exponential sums of $\mathcal{G}$ are Heilbronn sums, defined in Section 3. We derive

$$N_p(k) = J(p^2, \mathcal{G}, k, K) \ll \frac{k}{p} + \frac{k}{p^3} \sum_{w \in \mathbb{Z}_{p^2}} M_{p^2}(w; Z, \mathcal{G})(|H_p(w)| + 1). \qquad (8)$$

By the Hölder inequality, we obtain

$$\begin{aligned} &\left(\sum_{w \in \mathbb{Z}_{p^2}} M_{p^2}(w; Z, \mathcal{G}) |H_p(w)| \right)^4 \\ &\quad = \left(\sum_{w \in \mathbb{Z}_{p^2}} M_{p^2}(w; Z, \mathcal{G})^{1/2} (M_{p^2}(w; Z, \mathcal{G})^2)^{1/4} (|H_p(w)|^4)^{1/4} \right)^4 \\ &\quad \le \left(\sum_{w \in \mathbb{Z}_{p^2}} M_{p^2}(w; Z, \mathcal{G}) \right)^2 \sum_{w \in \mathbb{Z}_{p^2}} M_{p^2}(w; Z, \mathcal{G})^2 \sum_{w \in \mathbb{Z}_{p^2}} |H_p(w)|^4. \qquad (9) \end{aligned}$$

Trivially, we have

$$\sum_{w \in \mathbb{Z}_{p^2}} M_{p^2}(w; Z, \mathcal{G}) = 2\lfloor Z \rfloor (p-1) \ll p^{3+2\varepsilon} k^{-1}. \qquad (10)$$

We also see that

$$\sum_{w \in \mathbb{Z}_{p^2}} M_{p^2}(w; Z, \mathcal{G})^2 = (p-1) N(p^2, \mathcal{G}, Z).$$

We now choose

$$k = \lfloor p^{463/252 + 3\varepsilon} \rfloor.$$

Lemma 9 applies with $\nu = 6$ and leads to the estimate

$$\begin{aligned} N(p^2, \mathcal{G}, Z) &\le Z p^{13/84} (p^2)^{-1/14 + o(1)} + Z^2 p^{1/6} (p^2)^{-1/6 + o(1)} \\ &\le Z p^{13/84} (p^2)^{-1/14 + o(1)} \end{aligned}$$

(since for $Z \le p^{41/252}$ the first term dominates). Hence,

$$N(p^2, \mathcal{G}, Z) \le p^{2 + 1/84 + 3\varepsilon} k^{-1}.$$

Therefore

$$\sum_{w \in \mathbb{Z}_{p^2}} M_{p^2}(w; Z, \mathcal{G})^2 \ll p^{3 + 1/84 + 3\varepsilon} k^{-1}. \qquad (11)$$

Substituting (7), (10), and (11) in (9) and then using (8), we deduce that

$$\begin{aligned}N_p(k) &\ll \frac{k}{p} + \frac{k}{p^3}(p^{3+2\varepsilon}k^{-1})^{1/2}(p^{3+1/84+3\varepsilon}k^{-1})^{1/4}(p^{9/2})^{1/4} + p^{2\varepsilon}\\ &\ll \frac{k}{p} + k^{1/4}p^{127/336+2\varepsilon},\end{aligned}$$

provided p is large enough.

Recalling our choice of k, we see that

$$N_p(k) \ll \frac{k}{p} \tag{12}$$

for the preceding choice of k and sufficiently large p.

Since $a^{p-1} \equiv 1 \pmod{p^2}$ for all positive integers $a \le \ell_p$, this also holds for any a that is composed of primes $\ell \le \ell_p$. In particular it holds for any $a \in \mathcal{S}(k, \ell_p)$. Thus

$$\Psi(k, \ell_p) \le N_p(k). \tag{13}$$

Now, using Lemma 5 and the bound (12), we derive from (13) that

$$k^{1-\log\log k/\log \ell_p} \ll \frac{k}{p},$$

which implies that

$$\frac{\log\log k}{\log \ell_p} \ge \frac{\log p}{\log k} + O\left(\frac{1}{\log k}\right) = \left(\frac{463}{252} + 3\varepsilon\right)^{-1} + O\left(\frac{1}{\log p}\right).$$

Therefore

$$\begin{aligned}\log \ell_p &\le \left(\frac{463}{252} + 3\varepsilon\right)\log\log k + O\left(\frac{\log\log p}{\log p}\right)\\ &= \left(\frac{463}{252} + 3\varepsilon\right)\log\log p + O(1) \le \left(\frac{463}{252} + 4\varepsilon\right)\log\log p,\end{aligned}$$

provided that p is large enough. Taking into account that ε is arbitrary, we conclude the proof.

7. Proof of Theorem 3

7.1. Preliminaries

We need several statements about the groups of pth powers modulo p^2, which may be of independent interest.

Fix a prime p. Let again $\mathcal{G}$ be the group of order $p-1$, consisting of nonzero pth powers modulo p^2.

LEMMA 11. *If $n_1, n_2 \in \mathcal{G}$ are such that $n_1 \equiv n_2 \pmod{p}$ then we also have*

$$n_1 \equiv n_2 \pmod{p^2}.$$

Proof. Since $n_1, n_2 \in \mathcal{G}$ we can write

$$n_1 \equiv m_1^p \pmod{p^2} \quad \text{and} \quad n_2 \equiv m_2^p \pmod{p^2} \tag{14}$$

for some integers m_1 and m_2. Therefore

$$m_1 - m_2 \equiv m_1^p - m_2^p \equiv n_1 - n_2 \equiv 0 \pmod{p}.$$

Then $m_1 = m_2 + pk$ for some integer k, which, after substitution in (14), yields the desired congruence. □

For $v \in \mathbb{Z}_{p^2}$, let

$$\mathcal{D}_p(v) = \{(m_1, m_2) : 0 \le m_1, m_2 \le p-1,\ m_1^p - m_2^p \equiv v \pmod{p^2}\}. \tag{15}$$

We can rewrite Lemma 7 in the following form.

LEMMA 12. *Let $\mathcal{V}$ be a subset of $\mathbb{Z}_{p^2}^*$, $T = \#\mathcal{V}$, and $v_1/v_2 \notin \mathcal{G}$ for any distinct $v_1, v_2 \in \mathcal{V}$. Then*

$$\sum_{v \in \mathcal{V}} \#\mathcal{D}_p(v) \ll (pT)^{2/3}.$$

Proof. We follow the arguments of the proof of Lemma 2 from [10]. For $v \in \mathbb{Z}_{p^2}^*$ denote

$$\lambda(v) = v^{1-p} \in \mathbb{Z}_{p^2}^*.$$

Since the cardinality $\#\mathcal{D}_p(v)$ is invariant under multiplication by elements of the group $\mathcal{G}$ we have $\#\mathcal{D}_p(\lambda(v)) = \#\mathcal{D}_p(v)$. Next, we always have $\lambda(v) \equiv 1 \pmod{p}$. Therefore, the congruence

$$\lambda(v) \equiv m_1^p - m_2^p \pmod{p^2}$$

implies $m_1 - m_2 \equiv \lambda(v) \equiv 1 \pmod{p}$. Hence

$$\lambda(v) \equiv m_1^p - (m_1 - 1)^p \pmod{p^2}.$$

But

$$m_1^p - (m_1 - 1)^p \equiv 1 - pf(m_1) \pmod{p^2}$$

where the function $f(x)$ is defined by (5). Hence,

$$\#\mathcal{D}_p(v) = \#\mathcal{F}(U(v)) \tag{16}$$

where

$$U(v) = (1 - \lambda(v))/p \in \mathbb{Z}_p$$

and the set $\mathcal{F}(u)$ is defined by (6).

The assumption that $v_1/v_2 \notin \mathcal{G}$ for any distinct $v_1, v_2 \in \mathcal{V}$ implies $\lambda(v_1)/\lambda(v_2) \notin \mathcal{G}$ and $U(v_1) \ne U(v_2)$. Applying Lemma 7 to the set

$$U = \{U(v) : v \in \mathcal{V}\}$$

and using (16) we get

$$\sum_{v \in V} \#\mathcal{D}_p(v) = \sum_{u \in U} \#\mathcal{F}(u) \ll (pT)^{2/3}$$

as required. □

Now we consider two primes $p_1 \neq p_2$ and the corresponding subgroups $\mathcal{G}_\nu \subseteq \mathbb{Z}^*_{p_\nu^2}$ consisting of nonzero p_νth powers modulo p_ν^2, $\nu = 1, 2$.

Also, we denote by $\bar{\mathcal{G}}_\nu$ the subsets of $\mathbb{Z}$ formed by the integers belonging to $\mathcal{G}_\nu$ modulo p_ν^2. That is, while $\mathcal{G}_\nu$ is represented by some elements from the set $\{1, \dots, p_\nu^2 - 1\}$, the set $\bar{\mathcal{G}}_\nu$ is infinite, $\nu = 1, 2$.

Lemma 13. *Let x, K, and L be positive integers with $x < p_1^2 p_2^2$. Suppose that a set $\mathcal{A} \subseteq [1, x] \cap \bar{\mathcal{G}}_1 \cap \bar{\mathcal{G}}_2$ satisfies the following conditions*:

(i) *there are at least L pairs $(n_1, n_2) \in \mathcal{A}^2$ with $n_1 > n_2$ and such that $n_1 \equiv n_2 \pmod{p_2}$*;

(ii) *there are at most K elements of $\mathcal{A}$ in any residue class modulo p_1.*

Then

$$\frac{L}{K} \ll p_1^{2/3} Z^{1/3} N(p_1^2, \mathcal{G}_1, Z)^{1/3}$$

where $Z = \lfloor x/p_2^2 \rfloor$.

Proof. Denote

$$M_i = \#\{n \in \mathcal{A} : n - ip_2^2 \in \mathcal{A}\}, \quad i = 1, \dots, Z.$$

By Lemma 11 and the condition (i) we have

$$\sum_{i=1}^{Z} M_i \geq L.$$

Next, let

$$m_i = \#\{n \in \mathcal{G}_1 : n - ip_2^2 \in \mathcal{G}_1\}, \quad i = 1, \dots, Z.$$

Then by condition (ii) we have

$$\sum_{i=1}^{Z} m_i \geq \frac{1}{K} \sum_{i=1}^{Z} M_i \geq \frac{L}{K}. \tag{17}$$

We observe also that for $i = 1, \dots, Z$

$$m_i \leq \#\mathcal{D}_{p_1}(ip_2^2). \tag{18}$$

Moreover, we have $Z < p_1^2$. In particular, if a positive integer $i \leq Z$ is divisible by p_1 then, by Lemma 11,

$$m_i = \#\mathcal{D}_{p_1}(ip_2^2) = 0.$$

Assume that the residues of ip_2^2 modulo p_1^2, $i = 1, \dots, Z$, are contained in J distinct cosets $C_1, \dots, C_J$ of the group $\mathcal{G}_1$. For $j = 1, \dots, J$, we denote

$$s_j = \#\{i : 1 \leq i \leq Z,\ ip_2^2 \in C_j\}$$

and also

$$t_j = \#\mathcal{D}_{p_1}(v)$$

for some element $v \in C_j$ (clearly, this quantity depends only on the coset C_j and does not depend on the choice of v).

Therefore, using (18) we can rewrite (17) as

$$\sum_{j=1}^{J} s_j t_j \geq \frac{L}{K}. \tag{19}$$

To estimate the left-hand side of (19) from above we consider that the cosets $C_1, \ldots, C_J$ are ordered so that the sequence $\{t_1, \ldots, t_J\}$ is nonincreasing. By Lemma 12 we have for $j = 1, \ldots, J$

$$t_1 + \cdots + t_j \ll (p_1 j)^{2/3}.$$

Hence,

$$t_j \ll p_1^{2/3} j^{-1/3}. \tag{20}$$

Clearly,

$$\sum_{j=1}^{J} s_j = Z. \tag{21}$$

By the definition of $N(p_1^2, \mathcal{G}_1, Z)$, we have

$$\sum_{j=1}^{J} s_j^2 \leq N(p_1^2, \mathcal{G}_1, Z). \tag{22}$$

We notice that $Z \geq 1$; otherwise there are no $(n_1, n_2) \in \mathcal{A}^2$ with $n_1 > n_2$ and such that $n_1 \equiv n_2 \pmod{p_2}$. Define

$$J_0 = \lfloor Z^2/N(p_1^2, \mathcal{G}_1, Z) \rfloor \quad \text{and} \quad J_1 = \min\{J_0, J\}.$$

It is easy to see that $J_0 \geq 1$. Therefore, $J_1 \geq 1$.

To estimate the left-hand side of (19) we consider separately the cases $j \leq J_1$ and $j > J_1$ (the second case can occur only if $J_0 = J_1$). By (20), (22), and the Cauchy–Schwarz inequality, we have

$$\left(\sum_{j=1}^{J_1} s_j t_j \right)^2 \leq \sum_{j=1}^{J_1} s_j^2 \sum_{j=1}^{J_1} t_j^2 \leq \sum_{j=1}^{J} s_j^2 \sum_{j=1}^{J_0} t_j^2 \ll N(p_1^2, \mathcal{G}_1, Z) p_1^{4/3} J_0^{1/3}.$$

Therefore,

$$\sum_{j=1}^{J_1} s_j t_j \ll p_1^{2/3} Z^{1/3} N(p_1^2, \mathcal{G}_1, Z)^{1/3}. \tag{23}$$

If $J_0 = J_1$ then we also have to estimate the sum over $j > J_0$. To do so we use (20) and (21):

$$\sum_{j=J_0+1}^{J} s_j t_j \leq t_{J_0} Z \ll p_1^{2/3} Z^{1/3} N(p_1^2, \mathcal{G}_1, Z)^{1/3}. \tag{24}$$

Combining (19), (23), and (24), we complete the proof. □

Now we prove a combinatorial statement demonstrating that if a set $[1,x]\cap\bar{\mathcal{G}}_1\cap\bar{\mathcal{G}}_2$ is large then we can choose a set $\mathcal{A}\subseteq[1,x]\cap\bar{\mathcal{G}}_1\cap\bar{\mathcal{G}}_2$ satisfying the conditions of Lemma 13 with K and L such that $L/K\gg p_2$.

Let $\mathcal{I}_1$ and $\mathcal{I}_2$ be nonempty finite sets. For a set $\mathcal{A}\subseteq\mathcal{I}_1\times\mathcal{I}_2$ we denote the following horizontal and vertical "lines":

$$\mathcal{A}(x,\cdot)=\{y\in\mathcal{I}_2:(x,y)\in\mathcal{A}\};\qquad \mathcal{A}(\cdot,y)=\{x\in\mathcal{I}_1:(x,y)\in\mathcal{A}\}.$$

LEMMA 14. *For any set $\mathcal{A}\subseteq\mathcal{I}_1\times\mathcal{I}_2$ there exist a subset $\mathcal{B}\subseteq\mathcal{A}$ and positive integers k_1 and k_2 such that*:

(i) $\#\mathcal{B}\ge\frac{1}{2}\#\mathcal{A}$;

(ii) $\#\mathcal{B}(x,\cdot)\le k_1$ *for any* $x\in\mathcal{I}_1$;

(iii) $\#\mathcal{B}(\cdot,y)\le k_2$ *for any* $y\in\mathcal{I}_2$;

(iv) $$\sum_{\substack{x\in\mathcal{I}_1\\ \#\mathcal{B}(x,\cdot)>k_1/2}}\#\mathcal{B}(x,\cdot)\gg\frac{1}{\log(\#\mathcal{I}_1+\#\mathcal{I}_2)}\#\mathcal{A};$$

(v) $$\sum_{\substack{y\in\mathcal{I}_2\\ \#\mathcal{B}(\cdot,y)>k_2/2}}\#\mathcal{B}(\cdot,y)\gg\frac{1}{\log(\#\mathcal{I}_1+\#\mathcal{I}_2)}\#\mathcal{A}.$$

Proof. The case $\mathcal{A}=\emptyset$ is trivial, so we now consider that $\#\mathcal{A}>0$. Let U be the smallest integer such that $2^U\ge\#\mathcal{I}_1+\#\mathcal{I}_2$, so $1\le U\ll\log(\#\mathcal{I}_1+\#\mathcal{I}_2)$.

We construct the following sequence of sets $\{\mathcal{A}_\nu\}$, $\nu=0,1,\dots$. Set $\mathcal{A}_0=\mathcal{A}$. Assume that $\mathcal{A}_\nu$ has been constructed. We now define u_ν as the smallest integer u such that

$$\sum_{\substack{x\in\mathcal{I}_1\\ \#\mathcal{A}_\nu(x,\cdot)>2^u}}\#\mathcal{A}_\nu(x,\cdot)\le\frac{1}{8U}\#\mathcal{A}. \tag{25}$$

Similarly, let v_ν be the smallest integer v such that

$$\sum_{\substack{y\in\mathcal{I}_2\\ \#\mathcal{A}_\nu(\cdot,y)>2^v}}\#\mathcal{A}_\nu(\cdot,y)\le\frac{1}{8U}\#\mathcal{A}. \tag{26}$$

Define

$$\begin{aligned}\mathcal{A}_{\nu+1}=\mathcal{A}_\nu\setminus&\bigcup_{\substack{x\in\mathcal{I}_1\\ \#\mathcal{A}_\nu(x,\cdot)>2^{u_\nu}}}\{(x,y):y\in\mathcal{A}_\nu(x,\cdot)\}\\ \setminus&\bigcup_{\substack{y\in\mathcal{I}_2\\ \#\mathcal{A}_\nu(\cdot,y)>2^{v_\nu}}}\{(x,y):x\in\mathcal{A}_\nu(\cdot,y)\}.\end{aligned} \tag{27}$$

Clearly, for any $\nu=0,1,\dots$ we have

$$\mathcal{A}_{\nu+1}\subseteq\mathcal{A}_\nu,\quad 0\le u_{\nu+1}\le u_\nu<U,\quad 0\le v_{\nu+1}\le v_\nu<U.$$

There exists a number $N<2U$ such that

$$u_{N+1} = u_N \quad \text{and} \quad v_{N+1} = v_N.$$

Set

$$\mathcal{B} = \mathcal{A}_{N+1}, \quad k_1 = 2^{u_N}, \quad k_2 = 2^{v_N}.$$

Now, from (25), (26), and (27), we derive

$$\begin{aligned}
\#(\mathcal{A} \setminus \mathcal{B}) &\le \sum_{\nu=0}^{N} \sum_{\substack{x \in \mathcal{I}_1 \\ \#\mathcal{A}_\nu(x,\cdot) > 2^{u_\nu}}} \#\mathcal{A}_\nu(x,\cdot) + \sum_{\nu=0}^{N} \sum_{\substack{y \in \mathcal{I}_2 \\ \#\mathcal{A}(\cdot,y) > 2^{v_\nu}}} \#\mathcal{A}_\nu(\cdot,y) \\
&\le \frac{2(N+1)}{8U} \#\mathcal{A} \le \frac{1}{2} \#\mathcal{A}.
\end{aligned}$$

So, condition (i) is satisfied.

By the definition of $\mathcal{B}$, k_1, and k_2 we see that conditions (ii) and (iii) are satisfied too.

Next, if $k_1 = 1$ then

$$\sum_{\substack{x \in \mathcal{I}_1 \\ \#\mathcal{B}(x,\cdot) > k_1/2}} \#\mathcal{B}(x,\cdot) = \#\mathcal{B}.$$

If $k_1 > 1$ then we deduce from the equality $u_{N+1} = u_N$ that

$$\sum_{\substack{x \in \mathcal{I}_1 \\ \#\mathcal{B}(\cdot,y) > k_1/2}} \#\mathcal{B}(\cdot,y) > \frac{1}{8U} \#\mathcal{A}.$$

In either case the condition (iv) holds. Analogously, we also have condition (v) satisfied. □

7.2. *Conclusion of the Proof*

We suppose that Q is large enough while ε and δ are small enough and define

$$x = Q^{59/24 - 3\delta} \quad \text{and} \quad y = ((1-\delta)\log Q)^{59/35+\varepsilon}.$$

Assume that there are two primes $p_1 \ne p_2$ with $Q^{1-\delta} < p_1, p_2 \le Q$ and such that

$$a^{p_1 - 1} \equiv 1 \pmod{p_1^2}, \qquad a^{p_2 - 1} \equiv 1 \pmod{p_2^2}$$

for all positive integers $a \le y$.

As before, for $\nu = 1, 2$, we use $\mathcal{G}_\nu$ to denote the subgroup of $\mathbb{Z}_{p_\nu^2}^*$ consisting of nonzero p_νth powers modulo p_ν^2 and use $\bar{\mathcal{G}}_\nu$ for the subset of $\mathbb{Z}$ formed by the integers belonging to $\mathcal{G}_\nu$ modulo p_ν^2.

Then $\mathcal{S}(x, y) \subseteq \bar{\mathcal{G}}_1 \cap \bar{\mathcal{G}}_2$ (here we take into account that $y < \min\{p_1, p_2\}$). Since

$$(59/24 - 3\delta)\left(1 - \frac{1}{59/35 + \varepsilon}\right) > 1 + \delta$$

provided δ is small enough compared to ε, we derive from Lemma 5 that

$$\Psi(x, y) > Q^{1+\delta} \tag{28}$$

(provided ε and δ are small enough).

We now associate with any integer $n \in \mathcal{S}(x,y)$ the pair of residues

$$(n \pmod{p_1}, n \pmod{p_2}) \in \mathbb{Z}_{p_1} \times \mathbb{Z}_{p_2}.$$

Using Lemma 14 we conclude the existence of a set

$$\mathcal{A} \subseteq \mathcal{S}(x,y) \subseteq [1,x] \cap \bar{\mathcal{G}}_1 \cap \bar{\mathcal{G}}_2$$

and positive integers k_1, k_2 and an absolute constant c_0 satisfying the following conditions:

(a) $\#\mathcal{A} \geq \Psi(x,y)/2$;
(b) there are at most k_1 elements of $\mathcal{A}$ in any residue class modulo p_1;
(c) there are at most k_2 elements of $\mathcal{A}$ in any residue class modulo p_2;
(d) there are at least $c_0\Psi(x,y)/(k_1 \log Q)$ residue classes modulo p_1 containing at least $k_1/2$ elements from $\mathcal{A}$;
(e) there are at least $c_0\Psi(x,y)/(k_2 \log Q)$ residue classes modulo p_2 containing at least $k_2/2$ elements from $\mathcal{A}$.

Without loss of generality we can assume that $k_2 \geq k_1$.

In particular, we see from property (a) and (28) that

$$\#\mathcal{A} \gg Q^{1+\delta}.$$

Therefore, by properties (a) and (e) we have

$$Q \geq p_2 \geq c_0 \frac{\Psi(x,y)}{k_2 \log Q} \gg \frac{Q^{1+\delta}}{k_2 \log Q}.$$

Hence,

$$k_2 \gg \frac{Q^{\delta}}{\log Q},$$

provided that Q is large enough. If a residue class modulo p_2 contains at least $k_2/2$ elements from $\mathcal{A}$, then there are at least $k_2^2/10$ pairs $(n_1, n_2) \in \mathcal{A}^2$ such that $n_1 > n_2$ and $n_1 \equiv n_2 \pmod{p_2}$. Therefore, the conditions of Lemma 13 are fulfilled with $K = k_1$ and

$$L = \left\lceil \frac{k_2^2}{10} \right\rceil \times \left\lceil \frac{c_0\Psi(x,y)}{k_2 \log Q} \right\rceil \gg \frac{\Psi(x,y)k_2}{\log Q} \gg \frac{Q^{1+\delta}k_2}{\log Q}.$$

Considering again that Q is large enough we obtain that

$$\frac{L}{K} \geq \frac{k_2 Q}{k_1} \geq Q.$$

Applying Lemma 13, we obtain

$$p_1^{2/3} Z^{1/3} N(p_1^2, \mathcal{G}_1, Z)^{1/3} \gg Q \tag{29}$$

where

$$Z = \left\lfloor \frac{x}{p_2^2} \right\rfloor \leq Q^{11/24-\delta} \leq p_1^{11/24-\delta/2}.$$

On the other hand, Lemma 9 applies with $\nu = 2$ and yields

$$N(p_1^2, \mathcal{G}_1, Z) \le Z p_1^{5/12} (p_1^2)^{-1/6+o(1)} + Z^2 p_1^{1/2} (p_1^2)^{-1/2+o(1)} \le p_1^{13/24-\delta/2+o(1)}.$$

Consequently,

$$p_1^{2/3} Z^{1/3} N(p_1^2, \mathcal{G}_1, Z)^{1/3} \le p_1^{1-\delta/3+o(1)} \le Q^{1-\delta/3+o(1)},$$

which disagrees with (29) for Q large enough. This contradiction completes the proof.

8. Proof of Theorem 4

Let $\mathcal{P}_y$ be the set of all primes p for which

$$a^{p-1} \equiv 1 \pmod{p^2} \tag{30}$$

for all primes $a \le y$.

We need the following estimate, from which Theorem 4 follows quickly.

LEMMA 15. *Suppose $Q \ge 2y \ge 2$. Then for all $\delta > 0$ and any $x \ge 2$, we have*

$$\#\{p \in \mathcal{P}_y : Q/2 < p \le Q\} \ll \frac{(xQ)^\delta (Q^2 + xQ^{-1} + \min(xQ^{-1/2}, x^{1/2}Q))}{\Psi(x, y)}.$$

Proof. For real u, let

$$T(u) = \sum_{n \in \mathcal{S}(x,y)} \exp(2\pi i u n)$$

and put $Y = T(0) = \Psi(x, y)$.

Let $p \in \mathcal{P}_y$. By the Parseval identity, we have for each prime p

$$\begin{aligned}\sum_{\substack{a=1\\(a,p)=1}}^{p^2} \left|T\left(\frac{a}{p^2}\right)\right|^2 &= \sum_{a=1}^{p^2} \left|T\left(\frac{a}{p^2}\right)\right|^2 - \sum_{b=1}^{p} \left|T\left(\frac{b}{p}\right)\right|^2 \\ &= p^2 \sum_{a=1}^{p^2} N(p^2, a)^2 - p \sum_{b=1}^{p} N(p, b)^2, \end{aligned} \tag{31}$$

where $N(q, a)$ is the number of elements of $n \in \mathcal{S}(x, y)$ in the progression $n \equiv a \pmod{q}$. For $p \in \mathcal{P}_y$ we see that $n^{p-1} \equiv 1 \pmod{p^2}$ for every $n \in \mathcal{S}(x, y)$. By Lemma 11, for each $b \in \{1, \ldots, p-1\}$ there is a unique residue a_b modulo p^2 with $a_b \equiv b \pmod{p}$ and $a_b^{p-1} \equiv 1 \pmod{p}$. Consequently, $N(p^2, a_b) = N(p, b)$. Therefore

$$\sum_{a=1}^{p^2} N(p^2, a)^2 = \sum_{b=1}^{p} N(p^2, a_b)^2 = \sum_{b=1}^{p} N(p, b)^2,$$

which, after substitution in (31), implies that

$$\sum_{\substack{1 \le a \le p^2\\(a,p)=1}} \left|T\left(\frac{a}{p^2}\right)\right|^2 = p(p-1) \sum_{b=1}^{p} N(p, b)^2.$$

Since

$$\sum_{b=1}^{p} N(p,b) = Y$$

and clearly $N(p,0) = 0$ for $p > Q/2 \geq y$, by the Cauchy–Schwarz inequality, we obtain

$$\sum_{\substack{1\leq a\leq p^2\\(a,p)=1}} \left|T\left(\frac{a}{p^2}\right)\right|^2 = p(p-1)\sum_{b=1}^{p-1} N(p,b)^2 \geq pY^2.$$

Therefore

$$\sum_{\substack{p\in\mathcal{P}_y\\Q/2<p\leq Q}} \sum_{\substack{1\leq a\leq p^2\\(a,p)=1}} \left|T\left(\frac{a}{p^2}\right)\right|^2 \gg QY^2\#\{p\in\mathcal{P}_y : Q/2 < p \leq Q\}. \tag{32}$$

By Lemma 10,

$$\sum_{q\leq Q} \sum_{\substack{1\leq a\leq q^2\\(a,q)=1}} \left|T\left(\frac{a}{q^2}\right)\right|^2 \ll (xQ)^{\delta}(Q^3 + x + \min\{xQ^{1/2}, x^{1/2}Q^2\})Y. \tag{33}$$

Comparing (32) and (33), we obtain the desired estimate. □

To finish the proof of Theorem 4, we take $x = Q^{5/2}$ and $y = (\log Q)^{5/3+\varepsilon}$ in Lemma 15. Inserting the bound from Lemma 5, we have

$$\Psi(x,y) > x^{1-1/(5/3+\varepsilon)} \gg Q^{1+5\delta}$$

for a suitable $\delta > 0$. Therefore, for the previous choice of y we obtain

$$\#\{p\in\mathcal{P}_y : Q/2 < p \leq Q\} \ll Q^{1-\delta},$$

which implies the desired estimate.

9. Comments

Lemmas 6, 8, and 9 can easily be obtained in fully explicit forms with concrete constants. Thus, the bound of Theorem 1 can also be obtained in a fully explicit form, which can be important for algorithmic applications. For example, it would be interesting to get an explicit formula for $n_0(\varepsilon)$ such that for $n \geq n_0(\varepsilon)$ the conclusion of Corollary 2 holds.

It is interesting to establish the limits of our approach. For example, the bound

$$N_p(k) \ll kp^{-1+o(1)}$$

for values of $k = p^{1+o(1)}$ (or larger), which is the best possible result about $N_p(k)$, leads only to the estimate

$$\ell_p \leq (\log p)^{1+o(1)},$$

which is still much higher than the expected size of ℓ_p. Furthermore, if instead of Lemma 10 we have the best possible bound

$$\sum_{1 \le q \le Q} \sum_{\substack{a=1 \\ \gcd(a,q)=1}}^{q^2} \left| S\left(\frac{a}{q^2}\right) \right|^2 \ll Q^{\delta}(Q^3 + N)Y,$$

the exponent $5/3$ of Theorem 4 can be replaced with $3/2$.

Certainly, improving and obtaining unconditional variants of the estimate (3) and, more generally, investigating other properties of set $\mathcal{W}(p)$ is of great interest owing to important applications outlined in [12]. It is quite possible that Lemma 6 can be used for this purpose as well.

Congruences with Fermat quotients $q_p(a)$ modulo higher powers of p have also been considered in the literature; see [6; 13]. Using our approach with bounds of generalized Heilbronn sums

$$H_{p,m}(\lambda) = \sum_{b=1}^{p} \mathbf{e}_{p^m}(\lambda b^{p^{m-1}})$$

due to Bourgain and Chang [2] or Malykhin [17] (which is fully explicit), one can estimate the smallest a with

$$q_p(a) \not\equiv 1 \pmod{p^m}$$

for fixed $m \ge 2$.

References

[1] S. Baier and L. Zhao, *An improvement for the large sieve for square moduli,* J. Number Theory 128 (2008), 154–174.

[2] J. Bourgain and M.-C. Chang, *Exponential sum estimates over subgroups and almost subgroups of $\mathbb{Z}_Q^*$, where Q is composite with few prime factors,* Geom. Funct. Anal. 16 (2006), 327–366.

[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,* Internat. Math. Res. Notices (2008), 1–29.

[4] ———, *Corrigenda to: Product sets of rationals, multiplicative translates of subgroups in residue rings and fixed points of the discrete logarithm,* Internat. Math. Res. Notices (2009), 3146–3147.

[5] R. Crandall, K. Dilcher, and C. Pomerance, *A search for Wieferich and Wilson primes,* Math. Comp. 66 (1997), 433–449.

[6] R. Ernvall and T. Metsänkylä, *On the p-divisibility of Fermat quotients,* Math. Comp. 66 (1997), 1353–1365.

[7] W. L. Fouché, *On the Kummer–Mirimanoff congruences,* Quart. J. Math. Oxford Ser. (2) 37 (1986), 257–261.

[8] A. Granville, *Some conjectures related to Fermat's last theorem,* Number theory (Banff, 1988), pp. 177–192, de Gruyter, New York, 1990.

[9] ———, *On pairs of coprime integers with no large prime factors,* Exposition. Math. 9 (1991), 335–350.

[10] D. R. Heath-Brown and S. V. Konyagin, *New bounds for Gauss sums derived from kth powers, and for Heilbronn's exponential sum,* Quart. J. Math. Oxford Ser. (2) 51 (2000), 221–235.

[11] A. Hildebrand and G. Tenenbaum, *Integers without large prime factors,* J. Théor. Nombres Bordeaux 5 (1993), 411–484.
[12] Y. Ihara, *On the Euler–Kronecker constants of global fields and primes with small norms,* Algebraic geometry and number theory, Progr. Math., 850, pp. 407–451, Birkhäuser, Boston, 2006.
[13] W. Keller and J. Richstein, *Solutions of the congruence* $a^{p-1} \equiv 1 \pmod{p^r}$, Math. Comp. 74 (2005), 927–936.
[14] J. Knauerand and J. Richstein, *The continuing search for Wieferich primes,* Math. Comp. 74 (2005), 1559–1563.
[15] S.V. Konyagin and C. Pomerance, *On primes recognizable in deterministic polynomial time,* The mathematics of Paul Erdős, vol. I, pp. 176–198, Springer-Verlag, Berlin.
[16] H. W. Lenstra, *Miller's primality test,* Inform. Process. Lett. 8 (1979), 86–88.
[17] Y. V. Malykhin, *Estimates of trigonometric sums modulo* p^r, Mat. Zametki 80 (2006), 793–796 (Russian); English translation in Math. Notes 80 (2006), 748–752.

J. Bourgain
Institute for Advanced Study
Princeton, NJ 08540

bourgain@ias.edu

K. Ford
Department of Mathematics
University of Illinois
Urbana, IL 61801

ford@math.uiuc.edu

S. V. Konyagin
Department of Mechanics
and Mathematics
Moscow State University
Moscow 119992
Russia

konyagin@ok.ru

I. E. Shparlinski
Department of Computing
Macquarie University
Sydney, NSW 2109
Australia

igor.shparlinski@mq.edu.au