A PROBLEM IN COMPARATIVE ORDER THEORY

SERGEI KONYAGIN AND PAUL POLLACK

ABSTRACT. Write $\mathrm{ord}_p(\cdot)$ for the multiplicative order in $\mathbb{F}_p^\times$. Recently, Matthew Just and the second author investigated the problem of classifying pairs $\alpha, \beta \in \mathbb{Q}^\times \setminus \{\pm 1\}$ for which $\mathrm{ord}_p(\alpha) > \mathrm{ord}_p(\beta)$ holds for infinitely many primes p. They called such pairs order-dominant. We describe an easily-checkable sufficient condition for α, β to be order-dominant. Via the large sieve, we show that almost all integer pairs α, β satisfy our condition, with a power savings on the size of the exceptional set.

1. INTRODUCTION

For each rational prime p, we write $v_p(\cdot)$ for the p-adic valuation. If $\epsilon \in \mathbb{Q}_p$ with $v_p(\epsilon) = 0$, we let $\mathrm{ord}_p(\epsilon)$ denote the multiplicative order of ϵ in the residue ring $\mathbb{Z}_p/p\mathbb{Z}_p \cong \mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$. Now fix $\alpha, \beta \in \mathbb{Q}^\times \setminus \{\pm 1\}$. For all but finitely many primes p, both α and β are units in $\mathbb{Z}_p$, and so it is sensible to ask how $\mathrm{ord}_p(\alpha)$ and $\mathrm{ord}_p(\beta)$ compare, as p varies within the set of primes.

From results of Corrales-Rodrigañez and Schoof [4], if $\mathrm{ord}_p(\alpha) = \mathrm{ord}_p(\beta)$ for all but finitely many p, then $\alpha = \beta^{\pm 1}$. (Schinzel [9] had earlier obtained results in the same direction as [4] but less general.) In [10], Schinzel and Wójcik show that whenever $\alpha, \beta \in \mathbb{Q}^\times \setminus \{\pm 1\}$, there are infinitely many primes p with $v_p(\alpha) = v_p(\beta) = 0$ and $\mathrm{ord}_p(\alpha) = \mathrm{ord}_p(\beta)$. (Earlier, special cases of this result had been worked out — but not published — by J.S. Wilson, J.G. Thompson, and J.W.S. Cassels.) Inspired by these works, Just and the second author [7] recently investigated the following related question: For which pairs α, β are there infinitely many p with $v_p(\alpha) = v_p(\beta) = 0$ and $\mathrm{ord}_p(\alpha) > \mathrm{ord}_p(\beta)$? They termed such pairs order-dominant.

Under GRH, one can show that α, β is order-dominant as long as α is not a power of β. (When α and β are multiplicatively independent, a property stronger than order-dominance is proved, subject to GRH, by Järviniemi; see [8, Theorem 1.4]. The remaining cases are easier and do not need GRH.) In [7], Just and Pollack unconditionally establish order-dominance for several families of integer pairs A, B. A typical result of [7] is as follows: If A, B are odd positive integers, and the Jacobi symbol $\left(\frac{-B(1-B)}{A}\right) = -1$ or $\left(\frac{1-B}{A}\right) = -1$, then A, B is order dominant. Key to the proof of this and many of the other theorems of [7] is the following observation (implicit in work) of Banaszak [1].

Let $\alpha, \beta \in \mathbb{Q}^\times \setminus \{\pm 1\}$, and let p be an odd prime. Suppose that (a) α, β are units in $\mathbb{Z}_p$, (b) $v_p(\alpha^{2k} - \beta) \geq 1$ for some integer k, and (c) the Legendre symbol $\left(\frac{\alpha}{p}\right) = -1$. Condition (b) implies that β is a square mod p and that we have a containment of cyclic subgroups, $\langle \beta \bmod p \rangle \subseteq \langle \alpha \bmod p \rangle$. Since β is a square mod p while α is not (by (c)), $\alpha \bmod p \notin \langle \beta \bmod p \rangle$. Thus, $\langle \beta \bmod p \rangle \subsetneq \langle \alpha \bmod p \rangle$, and so $\mathrm{ord}_p(\beta) < \mathrm{ord}_p(\alpha)$. (In fact, we get slightly more from

---

this argument: $\mathrm{ord}_p(\alpha)/\mathrm{ord}_p(\beta)$ is a positive even integer.) Thus, if infinitely many primes p satisfy (a)–(c), then α, β is an order-dominant pair.

Let us call a pair α, β satisfying (a)–(c) for infinitely many p a **special pair**. Our main result is an easily-checkable criterion for α, β to be special.

Theorem 1.1. *Let $\alpha, \beta \in \mathbb{Q}^\times \setminus \{\pm 1\}$. Suppose there is an odd prime q for which*

(i) $v_q(\alpha) = v_q(\beta) = 0$,

(ii) *the Legendre symbol $\left(\frac{\alpha}{q}\right) = -1$,*

(iii) *there is an integer k with $v_q(\alpha^{2k} - \beta) \geq v_q(\alpha^{q-1} - 1)$.*

Then α, β is a special pair.

The authors of [7] report that they were unable to establish the order-dominance of the pair $17, 2$. That $17, 2$ is order-dominant (indeed, special) is an immediate consequence of Theorem 1.1: Take $q = 7$ and $k = 1$.

Probably α, β is special as long as α is not a rational square and $\mathbb{Q}(\sqrt{\alpha}) \neq \mathbb{Q}(\sqrt{\beta})$. These conditions are easily seen to be necessary. A simple computer program implementing the criterion of Theorem 1.1 verifies that these conditions are also sufficient for all integer pairs α, β with $1 < |\alpha|, |\beta| \leq 1000$. We do not know how to prove they are sufficient in general. Nevertheless, using the large sieve we can show that being "special" is actually rather ordinary: Almost all integer pairs are special.

Theorem 1.2. *For all large positive integers N, the number of non-special pairs of integers α, β with $1 < |\alpha|, |\beta| \leq N$ is $O(N^{3/2} \log N)$.*

Since α, β is non-special whenever α is a square, the upper bound of Theorem 1.2 is sharp up to the log factor.

2. Preliminaries

The following result is often referred to as the lemma on "Lifting the Exponent". We choose a formulation over $\mathbb{Z}_p$, but the proof is the same as over $\mathbb{Z}$ (see, for example, [3, Lemma 2.1.22, Corollary 2.1.23, p. 22]).

Lemma 2.1. *Let p be a prime number, and let $A \in \mathbb{Z}_p$ with $v_p(A - 1) \geq 1$. Then*

$$v_p(A^n - 1) \geq v_p(A - 1) + v_p(n)$$

for every integer n. Furthermore, equality holds whenever p is odd.

Lemma 2.2. *Let p be an odd prime. Let $A \in \mathbb{Z}_p$ with $v_p(A - 1) = t \geq 1$. For each integer $T \geq t$, and each $B \in \mathbb{Z}_p$ with $B \equiv 1 \pmod{p^t}$, there is an integer n with*

$$A^n \equiv B \pmod{p^T}.$$

Proof. Since $v_p(A - 1) \geq 1$, we have $v_p(A) = 0$, so that A is invertible in $\mathbb{Z}_p$. For every pair of integers n and n',

$$A^n \equiv A^{n'} \pmod{p^T} \iff A^{n-n'} \equiv 1 \pmod{p^T} \iff n \equiv n' \pmod{p^{T-t}},$$

using Lemma 2.1 for the final equivalence. It follows that $A \bmod p^T$ generates a subgroup of $(\mathbb{Z}_p/p^T\mathbb{Z}_p)^\times$ of order p^{T-t}. Since each power of A is congruent to 1 mod p^t, and there are only p^{T-t} elements mod p^T congruent to 1 mod p^t, the result follows. $\qquad\square$

The proof of Theorem 1.1 relies crucially on the quadratic reciprocity law. Let d be a nonzero integer. If $\gamma \in \mathbb{Q}^\times$ and $v_p(\gamma) = 0$ for all $p \mid 2d$, we define the generalized Jacobi symbol

$$\left(\frac{d}{\gamma}\right) := \prod_{p:\ v_p(\gamma) \neq 0} \left(\frac{d}{p}\right)^{v_p(\gamma)},$$

where each $\left(\frac{d}{p}\right)$ is a Legendre symbol.

Lemma 2.3. *Let d be a nonzero integer, and let $\eta \in \mathbb{Q}_{>0}$. Suppose that*

$$v_p(\eta - 1) \geq 1 \qquad \text{for all odd primes } p \mid d$$

and that

$$v_2(\eta - 1) \geq 3.$$

Then $\left(\frac{d}{\eta}\right) = 1$.

Proof. This is a consequence of quadratic reciprocity, viewed as a special case of Artin's reciprocity law. A down-to-earth proof is as follows: We may write $\eta = P/Q$ where P, Q are positive integers coprime to each other and each coprime to $2d$. Then $\left(\frac{d}{\eta}\right) = \left(\frac{d}{P}\right)\left(\frac{d}{Q}\right) = \left(\frac{\Delta}{P}\right)\left(\frac{\Delta}{Q}\right)$, where Δ is the discriminant of $\mathbb{Q}(\sqrt{d})$. The conditions on the valuations of $\eta - 1$ imply that $P \equiv Q \pmod{\Delta}$. The desired result follows from recalling that the Kronecker symbol $\left(\frac{\Delta}{\cdot}\right)$ is a Dirichlet character modulo $|\Delta|$ (see [3, Theorem 2.2.9, p. 38]), so that $\left(\frac{\Delta}{P}\right) = \left(\frac{\Delta}{Q}\right)$ and $\left(\frac{\Delta}{P}\right)\left(\frac{\Delta}{Q}\right) = (\pm 1)^2 = 1$. $\qquad\square$

Finally, we recall Bombieri's form of the arithmetic large sieve (see [2, Theorem 1]).

Proposition 2.4. *Let N be a positive integer, and let $\mathcal{N}$ be a subset of $[-N, N]$. Set $Z := \#\mathcal{N}$. For each prime $p \leq \sqrt{N}$ and each integer h, let $Z(p, h) = \#\{n \in \mathcal{N} : n \equiv h \pmod{p}\}$. Then*

$$\sum_{p \leq \sqrt{N}} p \sum_{h \bmod p} \left(Z(p, h) - \frac{Z}{p}\right)^2 \ll NZ.$$

3. Proof of Theorem 1.1

By replacing α with $1/\alpha$, we can (and will) assume that $|\alpha| > 1$. Our task is to show that the set

$$\mathcal{P} = \{\text{odd primes } p : v_p(\alpha) = v_p(\beta) = 0, \left(\frac{\alpha}{p}\right) = -1, \beta \bmod p \in \langle \alpha^2 \bmod p \rangle\}$$

is infinite.

We suppose for a contradiction that $\mathcal{P}$ is finite. Note that $\mathcal{P}$ is nonempty since $q \in \mathcal{P}$.

Since the details of the proof are somewhat intricate, we first give the basic idea. Let d be the unique squarefree integer differing from α by the square of a rational number. We will consider the generalized Jacobi symbol $\left(\frac{d}{\eta}\right)$, where $\eta := \frac{\alpha^{2K'} - \beta}{\alpha^{2K} - \beta}$ for well-chosen integers K and K'. On the one hand, the reciprocity law in the form of Lemma 2.3 will imply that $\left(\frac{d}{\eta}\right) = 1$. On the other hand, by controlling the power of q appearing in the factorizations of $\alpha^{2K'} - \beta$ and $\alpha^{2K} - \beta$, we will be able, using $\left(\frac{d}{q}\right) = \left(\frac{\alpha}{q}\right) = -1$, to force $\left(\frac{d}{\eta}\right) = -1$.

Now down to business. Put $e := v_q(\alpha^{q-1} - 1)$. Setting
$$\ell = \mathrm{ord}_q(\alpha^2),$$
we observe that $\ell \mid \frac{q-1}{2}$. By Lemma 2.1,
$$e = v_q((\alpha^{2\ell})^{(q-1)/2\ell} - 1)$$
$$= v_q(\alpha^{2\ell} - 1).$$

By assumption (iii), we may choose an integer k with
$$v_q(\alpha^{2k} - \beta) \geq e.$$

Adjusting k by a multiple of $\phi(q^e)$, we can assume that k is large. Concretely, we assume that
$$\alpha^{2k} - \beta > 0$$
and that

(1) $$k \geq 3 + \max_p |v_p(\beta)|,$$

where the maximum is taken over all primes p.

Let
$$e' = v_q(\alpha^{2k} - \beta),$$
and define
$$M = q^{e'} \prod_{\substack{p \in \mathcal{P} \\ p \neq q}} (p-1) \prod_{p:\ v_p(\alpha) \neq 0} (p-1).$$

Put
$$e'' = v_q(M),$$
so that $e'' \geq e' \geq e$. Viewing the rational numbers with denominator prime to q as embedded in $\mathbb{Z}_q$, we may write
$$\alpha^{2k} = \beta(1 + q^{e'}\epsilon),$$
where $\epsilon \in \mathbb{Z}_q^\times$. Choose a positive integer n_0 such that
$$(\alpha^{2\ell})^{n_0} \equiv \frac{1 + q^{e+e''}}{1 + q^{e'}\epsilon} \pmod{q^{e+e''+1}};$$

this is possible by Lemma 2.2 (with $A = \alpha^{2\ell}$), since $v_q(\alpha^{2\ell} - 1) = e$ and $\frac{1+q^{e+e''}}{1+q^{e'}\epsilon} \equiv 1 \pmod{q^e}$. Then
$$v_q(\alpha^{2(k+\ell n_0)} - \beta) = e + e''.$$

We set $K = k + \ell n_0$; this is the integer K described in our initial proof summary. We proceed to choose K'.

For $p \in \mathcal{P}$, $p \neq q$, we let f_p be the integer determined by the factorization

$$\alpha^{2(k+\ell n_0)} - \beta = \left(q^{e+e''} \prod_{\substack{p \in \mathcal{P} \\ p \neq q}} p^{f_p} \right) R,$$

where $v_p(R) = 0$ for all $p \in \mathcal{P}$. If $v_2(\alpha) = v_2(\beta) = 0$, we further define

$$f_2 = v_2(\alpha^{2(k+\ell n_0)} - \beta).$$

Let

$$N = 2M \left(\prod_{\substack{p \in \mathcal{P} \\ p \neq q}} p^{f_p} \right) \cdot \widetilde{2^{f_2}},$$

where the tilde indicates that the final term is included only when $v_2(\alpha) = v_2(\beta) = 0$. Then $v_q(N) = v_q(M) = e''$, so that by Lemma 2.1,

$$v_q(\alpha^{2\ell N} - 1) = v_q(\alpha^{2\ell} - 1) + v_q(N)$$
$$= e + e''.$$

Now writing

$$\alpha^{2(k+\ell n_0)} = \beta(1 + q^{e+e''}\gamma),$$

where $\gamma \in \mathbb{Z}_q^\times$, we use Lemma 2.2 (with $A = \alpha^{2\ell N}$) to choose a positive integer n_1 such that

$$\alpha^{2\ell N n_1} \equiv \frac{1 + q^{e+e''+1}}{1 + q^{e+e''}\gamma} \pmod{q^{e+e''+2}}.$$

(This is possible, since the right-hand side of the congruence is 1 mod $q^{e+e''}$.) Then

$$v_q(\alpha^{2(k+\ell n_0 + \ell N n_1)} - \beta) = e + e'' + 1.$$

We take $K' := k + \ell n_0 + \ell N n_1$.

We proceed to compare the factorizations of $\alpha^{2K} - \beta$ and $\alpha^{2K'} - \beta$. Let $p \in \mathcal{P} \setminus \{q\}$, allowing also $p = 2$ if $v_2(\alpha) = v_2(\beta) = 0$. By construction, $\phi(p^{f_p+1}) \mid N$. Thus, $\alpha^{2\ell N n_1} \equiv 1 \pmod{p^{f_p+1}}$, and so

$$v_p(\alpha^{2(k+\ell n_0 + \ell N n_1)} - \beta) = v_p((\alpha^{2\ell N n_1} - 1)\alpha^{2(k+\ell n_0)} + (\alpha^{2(k+\ell n_0)} - \beta)) = v_p(\alpha^{2(k+\ell n_0)} - \beta)$$

by the ultrametric inequality, since

$$f_p = v_p(\alpha^{2(k+\ell n_0)} - \beta) < v_p(\alpha^{2\ell N n_1} - 1).$$

It follows that the ratio

(2) $$\frac{\alpha^{2K'} - \beta}{\alpha^{2K} - \beta} = \frac{\alpha^{2(k+\ell n_0 + \ell N n_1)} - \beta}{\alpha^{2(k+\ell n_0)} - \beta} = qS,$$

where $v_p(S) = 0$ for all $p \in \mathcal{P}$, $p \neq q$, and also $v_2(S) = 0$ when $v_2(\alpha) = v_2(\beta) = 0$.

Let us examine the factorization of S. Let p be a prime, and suppose to start with that $v_p(\alpha) < 0$. By the ultrametric inequality and (1), $v_p(\alpha^{2K'} - \beta) = 2K'v_p(\alpha)$ while $v_p(\alpha^{2K} - \beta) = 2Kv_p(\alpha)$. Hence,

$$v_p(S) = 2(K' - K)v_p(\alpha) = 2\ell N n_1 v_p(\alpha).$$

If instead $v_p(\alpha) > 0$, then $v_p(\alpha^{2K'} - \beta) = v_p(\beta) = v_p(\alpha^{2K} - \beta)$, so that $v_p(S) = 0$. Finally, suppose that $v_p(\alpha) = 0$. If $v_p(\beta) > 0$, then $v_p(\alpha^{2K'} - \beta) = 0 = v_p(\alpha^{2K} - \beta)$, while if $v_p(\beta) < 0$, then $v_p(\alpha^{2K'} - \beta) = v_p(\beta) = v_p(\alpha^{2K} - \beta)$; in both cases, $v_p(S) = 0$. Hence, if $v_p(\alpha) = 0$ and $v_p(S) \neq 0$, then $v_p(\beta) = 0$. If $v_p(\alpha) = v_p(\beta) = 0$ and $v_p(S) \neq 0$, we know from the last paragraph that p is odd and not in $\mathcal{P}$. Since $v_p(S) \neq 0$, it must be that $v_p(\alpha^{2K'} - \beta) > 0$ or $v_p(\alpha^{2K} - \beta) > 0$; in either case, $\beta \bmod p$ lands in the multiplicative group generated by $\alpha^2 \bmod p$. So in order to have $p \notin \mathcal{P}$, it must be that $\left(\frac{\alpha}{p}\right) = 1$. We conclude (since $S > 0$) that S admits a factorization

$$S = \prod_{p:\ v_p(\alpha)<0} p^{2\ell N n_1 v_p(\alpha)} \prod_{\substack{p \text{ odd} \\ v_p(\alpha)=v_p(\beta)=0 \\ \left(\frac{\alpha}{p}\right)=1}} p^{v_p(S)}.$$

Comparing the last display with (2), we find upon rearranging that

$$\frac{(\alpha \prod_{p:\ v_p(\alpha)<0} p^{-v_p(\alpha)})^{2K'} - \beta(\prod_{p:\ v_p(\alpha)<0} p^{-v_p(\alpha)})^{2K'}}{(\alpha \prod_{p:\ v_p(\alpha)<0} p^{-v_p(\alpha)})^{2K} - \beta(\prod_{p:\ v_p(\alpha)<0} p^{-v_p(\alpha)})^{2K}} = q \prod_{\substack{p \text{ odd} \\ v_p(\alpha)=v_p(\beta)=0 \\ \left(\frac{\alpha}{p}\right)=1}} p^{v_p(S)}.$$

For notional convenience, we let η denote the fractional expression on the left-hand side, and we write μ, ν for its numerator and denominator, respectively.

Recall that d is the squarefree integer for which $d(\mathbb{Q}^\times)^2 = \alpha(\mathbb{Q}^\times)^2$. Notice that with this choice of d, whenever p is a prime for which $v_p(\alpha) = 0$, also $v_p(d) = 0$ and (if p is odd) $\left(\frac{\alpha}{p}\right) = \left(\frac{d}{p}\right)$.

We evaluate $\left(\frac{d}{\eta}\right)$ in two different ways. On the one hand, since $\left(\frac{\alpha}{q}\right) = -1$,

$$\left(\frac{d}{\eta}\right) = \left(\frac{d}{q}\right) \prod_{\substack{p \text{ odd} \\ v_p(\alpha)=v_p(\beta)=0 \\ \left(\frac{\alpha}{p}\right)=1}} \left(\frac{d}{p}\right)^{v_p(S)} = \left(\frac{\alpha}{q}\right) \prod_{\substack{p \text{ odd} \\ v_p(\alpha)=v_p(\beta)=0 \\ \left(\frac{\alpha}{p}\right)=1}} \left(\frac{\alpha}{p}\right)^{v_p(S)} = -1.$$

On the other hand, we can show $\left(\frac{d}{\eta}\right) = 1$ by verifying the conditions of Lemma 2.3. Let p be an odd prime dividing d; then either $v_p(\alpha) < 0$ or $v_p(\alpha) > 0$. Suppose first that $v_p(\alpha) < 0$. Then the ultrametric inequality and (1) imply that $v_p(\mu) = v_p(\nu) = 0$. Write

$$(3) \quad \nu - \mu = \left(\alpha \prod_{p:\ v_p(\alpha)<0} p^{-v_p(\alpha)}\right)^{2K} \left((\alpha \prod_{p:\ v_p(\alpha)<0} p^{-v_p(\alpha)})^{2\ell N n_1} - 1\right)$$

$$+ \beta\left(\prod_{p:\ v_p(\alpha)<0} p^{-v_p(\alpha)}\right)^{2K} \left(1 - (\prod_{p:\ v_p(\alpha)<0} p^{-v_p(\alpha)})^{2\ell N n_1}\right).$$

This difference has positive p-adic valuation: Indeed, since $p - 1 \mid M \mid N$,

$$v_p\Big((\alpha \prod_{p:\ v_p(\alpha)<0} p^{-v_p(\alpha)})^{2\ell N n_1} - 1\Big) \geq 1$$

while also (from (1))

$$v_p\Big(\beta\Big(\prod_{p:\ v_p(\alpha)<0} p^{-v_p(\alpha)}\Big)^{2K}\Big) = v_p(\beta) + 2K|v_p(\alpha)| > v_p(\beta) + k > 0.$$

Hence, $v_p(\eta - 1) = v_p(\frac{\mu}{\nu} - 1) = v_p(\mu - \nu) > 0$. Suppose instead that $v_p(\alpha) > 0$. In this case, $v_p(\nu) = v_p(\beta)$. Also,

$$v_p\Big(\Big(\alpha \prod_{p:\ v_p(\alpha)<0} p^{-v_p(\alpha)}\Big)^{2K}\Big) = 2K v_p(\alpha) > k > v_p(\beta)$$

while

$$v_p\Big(\beta\Big(1 - (\prod_{p:\ v_p(\alpha)<0} p^{-v_p(\alpha)})^{2\ell N n_1}\Big)\Big) = v_p(\beta) + v_p\Big(1 - (\prod_{p:\ v_p(\alpha)<0} p^{-v_p(\alpha)})^{2\ell N n_1}\Big)$$
$$> v_p(\beta),$$

using for the last inequality that $p - 1 \mid M \mid N$. From (3), $v_p(\mu - \nu) > v_p(\beta)$ and $v_p(\eta - 1) = v_p(\mu - \nu) - v_p(\nu) = v_p(\mu - \nu) - v_p(\beta) \geq 1$.

It remains (only) to check that $v_2(\eta - 1) \geq 3$. If $v_2(\alpha) > 0$, then $v_2(\nu) = v_2(\beta)$. Moreover,

$$v_2\Big(\Big(\alpha \prod_{p:\ v_p(\alpha)<0} p^{-v_p(\alpha)}\Big)^{2K}\Big) = 2K v_2(\alpha) > k \geq 3 + v_2(\beta)$$

by (1), while

$$v_2\Big(\beta\Big(1 - (\prod_{p:\ v_p(\alpha)<0} p^{-v_p(\alpha)})^{2\ell N n_1}\Big)\Big) = v_2(\beta) + v_2\Big(1 - (\prod_{p:\ v_p(\alpha)<0} p^{-v_p(\alpha)})^{2\ell N n_1}\Big)$$
$$\geq 3 + v_2(\beta),$$

using for the last inequality that squares of 2-adic units are 1 mod 8. So from (3), $v_2(\mu - \nu) \geq 3 + v_2(\beta)$ and $v_2(\eta - 1) \geq 3$. Now suppose that $v_2(\alpha) < 0$. Then $v_2(\mu) = v_2(\nu) = 0$. Also,

$$v_2\Big((\alpha \prod_{p:\ v_p(\alpha)<0} p^{-v_p(\alpha)})^{2\ell N n_1} - 1\Big) \geq 3$$

while

$$v_2\Big(\beta\Big(\prod_{p:\ v_p(\alpha)<0} p^{-v_p(\alpha)}\Big)^{2K}\Big) = v_2(\beta) + 2K|v_2(\alpha)| > v_2(\beta) + k \geq 3.$$

Hence, $v_2(\eta - 1) = v_2(\mu - \nu) \geq 3$ in this case. Finally, suppose that $v_2(\alpha) = 0$. Write

$$\eta = \frac{\alpha^{2K'} - \beta}{\alpha^{2K} - \beta} \prod_{p:\ v_p(\alpha)<0} p^{-2\ell N n_1 v_p(\alpha)},$$

so that

$$\eta - 1 = \left(\frac{\alpha^{2K'} - \beta}{\alpha^{2K} - \beta} - 1\right)\left(\prod_{p:\ v_p(\alpha)<0} p^{-2\ell N n_1 v_p(\alpha)} - 1\right)$$

$$+ \left(\prod_{p:\ v_p(\alpha)<0} p^{-2\ell N n_1 v_p(\alpha)} - 1\right) + \left(\frac{\alpha^{2K'} - \beta}{\alpha^{2K} - \beta} - 1\right).$$

Since $v_2(\prod_{p:\ v_p(\alpha)<0} p^{-2\ell N n_1 v_p(\alpha)} - 1) \geq 3$, the desired inequality $v_2(\eta - 1) \geq 3$ will follow once it is shown that $v_2(\frac{\alpha^{2K'} - \beta}{\alpha^{2K} - \beta} - 1) \geq 3$. We have

$$v_2\left(\frac{\alpha^{2K'} - \beta}{\alpha^{2K} - \beta} - 1\right) = v_2(\alpha^{2(K'-K)} - 1) - v_2(\alpha^{2K} - \beta).$$

If $v_2(\beta) < 0$ or $v_2(\beta) > 0$, then $v_2(\alpha^{2k} - \beta) = v_2(\beta)$ or $v_2(\alpha^{2k} - \beta) = 0$ (respectively); in either case, the inequality $v_2(\frac{\alpha^{2K'} - \beta}{\alpha^{2K} - \beta} - 1) \geq 3$ follows from $v_2(\alpha^{2(K'-K)} - 1) \geq 3$. So we may suppose that $v_2(\beta) = 0$. In this case, we use that $2^{f_2} \mid N$. (Recall that $f_2 = v_2(\alpha^{2K} - \beta)$.) Since

$$v_2(\alpha^{2\ell n_1} - 1) \geq 3,$$

Lemma 2.1 (with $A = \alpha^{2\ell n_1}$) shows that

$$v_2(\alpha^{2(K'-K)} - 1) = v_2(\alpha^{2\ell N n_1} - 1) \geq 3 + v_2(N) \geq 3 + f_2,$$

so that

$$v_2(\alpha^{2(K'-K)} - 1) - v_2(\alpha^{2K} - \beta) \geq (3 + f_2) - f_2 = 3.$$

This completes the proof of Theorem 1.1.

4. Proof of Theorem 1.2

We start with an overview of the proof, deferring details to §§4.1–4.3 below.

Let N be an integer, $N \geq 2$. Let $\mathcal{B}$ denote the collection of nonzero integers $\beta \in [-N, N]$ that **do not** obey the following hypothesis.

Hypothesis 4.1. *There are more than $\frac{1}{4}\sqrt{N}/\log N$ primes $q \in (\frac{1}{2}\sqrt{N}, \sqrt{N}]$ with $\left(\frac{\beta}{q}\right) = 1$.*

For large enough N, one expects that $\mathcal{B}$ is empty (as would follow from GRH). Proving $\mathcal{B}$ is empty seems quite difficult (see [5] for a discussion of related problems), but for our purposes it is enough to know that $\mathcal{B}$ is fairly small. We prove in §4.1 that

$$(4) \qquad\qquad\qquad\qquad \#\mathcal{B} \ll N^{1/2} \log N.$$

Now fix an integer β with $1 < |\beta| \leq N$ and $\beta \notin \mathcal{B}$. For each integer α, let $\mathcal{P}(\alpha)$ denote the set of odd primes $q \in (\frac{1}{2}\sqrt{N}, \sqrt{N}]$ for which

(1) $\left(\frac{\beta}{q}\right) = 1$,

(2) α is a primitive root modulo q.

If there is any $q \in \mathcal{P}(\alpha)$ for which $v_q(\alpha^{q-1} - 1) = 1$, we can deduce from Theorem 1.1 (applied with this q) that α, β is special. Indeed, conditions (i) and (ii) of Theorem 1.1 are obvious. Since α^2 generates the subgroup of nonzero squares mod q, we can choose k with $\alpha^{2k} \equiv \beta$ (mod q). Then $v_q(\alpha^{2k} - \beta) \geq 1 = v_q(\alpha^{q-1} - 1)$, and so we have (iii).

In §§4.2–4.3 we show there is a $q \in \mathcal{P}(\alpha)$ with $v_q(\alpha^{q-1} - 1) = 1$ for every $\alpha \in [-N, N]$, apart from at most $O(N^{1/2} \log N)$ exceptions. Putting this together with our bound (4) on $\#\mathcal{B}$, we find that the number of non-special integer pairs α, β with $1 < |\alpha|, |\beta| \leq N$ is

$$\ll N \cdot N^{1/2} \log N + N^{1/2} \log N \cdot N \ll N^{3/2} \log N,$$

as claimed in Theorem 1.2.

4.1. **Bounding $\#\mathcal{B}$.** Let $Q = \pi(\sqrt{N}) - \pi(\frac{1}{2}\sqrt{N})$, so that $Q \sim \sqrt{N}/\log N$ as $N \to \infty$. For each integer β, put $S_\beta = \sum_{q \in (\frac{1}{2}\sqrt{N}, \sqrt{N}]} \left(\frac{\beta}{q}\right)$. If $\beta \in \mathcal{B}$, then (assuming N is large)

$$S_\beta + Q = \sum_{q \in (\frac{1}{2}\sqrt{N}, \sqrt{N}]} \left(1 + \left(\frac{\beta}{q}\right)\right) \leq 2 \cdot \frac{1}{4}\sqrt{N}/\log N + \#\{q \in (\frac{1}{2}\sqrt{N}, \sqrt{N}] : q \mid \beta\}$$

$$\leq \frac{1}{2}\sqrt{N}/\log N + 2 < \frac{2}{3}Q,$$

so that $S_\beta < -\frac{1}{3}Q$. It follows that

(5) $$\sum_{|\beta| \leq N} S_\beta^2 \gg Q^2 \#\mathcal{B}.$$

On the other hand, $\sum_{|\beta| \leq N} S_\beta^2 = S_1 + S_2$, where

$$S_1 = \sum_{q \in (\frac{1}{2}\sqrt{N}, \sqrt{N}]} \sum_{|\beta| \leq N} \left(\frac{\beta}{q}\right)^2, \quad \text{and} \quad S_2 = \sum_{|\beta| \leq N} \sum_{\substack{q_1, q_2 \in (\frac{1}{2}\sqrt{N}, \sqrt{N}] \\ q_1 \neq q_2}} \left(\frac{\beta}{q_1 q_2}\right).$$

When $q_1 \neq q_2$, the Jacobi symbol $\left(\frac{\cdot}{q_1 q_2}\right)$ is a nontrivial character mod $q_1 q_2$, and the Pólya–Vinogradov inequality yields

$$S_2 = \sum_{\substack{q_1, q_2 \in (\frac{1}{2}\sqrt{N}, \sqrt{N}] \\ q_1 \neq q_2}} \sum_{|\beta| \leq N} \left(\frac{\beta}{q_1 q_2}\right) \ll \sum_{\substack{q_1, q_2 \in (\frac{1}{2}\sqrt{N}, \sqrt{N}] \\ q_1 \neq q_2}} \sqrt{q_1 q_2} \log(q_1 q_2) \ll Q^2 N^{1/2} \log N.$$

Trivially, $S_1 \ll QN$, and a straightforward check shows $QN \ll Q^2 N^{1/2} \log N$. Hence, $\sum_{|\beta| \leq N} S_\beta^2 \ll Q^2 N^{1/2} \log N$. The desired bound $\#\mathcal{B} \ll N^{1/2} \log N$ follows by comparison with (5).

4.2. **Estimating $\#\mathcal{P}(\alpha)$.** For the remainder of the proof, β is a fixed integer with $1 < |\beta| \leq N$ and $\beta \notin \mathcal{B}$.

Recall that $\mathcal{P}(\alpha)$ denotes the set of primes $q \in (\frac{1}{2}\sqrt{N}, N]$ for which $\left(\frac{\beta}{q}\right) = 1$ and α is a primitive root mod q. Let us argue that there is an absolute constant $c_1 > 0$ such that

$$\#\mathcal{P}(\alpha) > c_1 \sqrt{N}/\log N$$

for all but $O(N^{1/2} \log N)$ integers $\alpha \in [-N, N]$.

Write $\mathcal{P}_0$ for the set of primes $q \in (\frac{1}{2}\sqrt{N}, \sqrt{N}]$ with $\left(\frac{\beta}{q}\right) = 1$. Since $\beta \notin \mathcal{B}$, we have $\#\mathcal{P}_0 > \frac{1}{4}\sqrt{N}/\log N$. It will be helpful momentarily to have a lower bound on $\sum_{q \in \mathcal{P}_0} \phi(q-1)/q$. For this we borrow an argument of Gallagher [6, p. 17]: By Cauchy–Schwarz,

$$\sum_{q \in \mathcal{P}_0} \frac{\phi(q-1)}{q} \sum_{q \in \mathcal{P}_0} \frac{q}{\phi(q-1)} \geq (\#\mathcal{P}_0)^2 > \frac{1}{16}N/(\log N)^2,$$

while (see eq. (10) of [6]) for a certain absolute positive constant c_2,

$$\sum_{q \in \mathcal{P}_0} \frac{q}{\phi(q-1)} \leq 2 \sum_{q \leq \sqrt{N}} \frac{q-1}{\phi(q-1)} \leq c_2 \sqrt{N}/\log N.$$

Hence, $\sum_{q \in \mathcal{P}_0} \phi(q-1)/q \geq c_3 \sqrt{N}/\log N$ for an absolute constant $c_3 > 0$.

Let $\mathcal{N}$ be the set of integers $\alpha \in [-N, N]$ with $\#\mathcal{P}(\alpha) \leq \frac{1}{2}c_3\sqrt{N}/\log N$. We apply the large sieve (Proposition 2.4) to estimate $Z = \#\mathcal{N}$. Observe that

$$\sum_{\substack{q \in \mathcal{P}_0}} \sum_{\substack{h \bmod q \\ h \text{ generates } \mathbb{F}_q^\times}} Z(q, h) = \sum_{q \in \mathcal{P}_0} \sum_{\alpha \in \mathcal{N}} 1_{\alpha \text{ prim. root mod } q}$$

$$= \sum_{\alpha \in \mathcal{N}} \#\mathcal{P}(\alpha) \leq \frac{1}{2}c_3 Z\sqrt{N}/\log N.$$

On the other hand,

$$\sum_{\substack{q \in \mathcal{P}_0}} \sum_{\substack{h \bmod q \\ h \text{ generates } \mathbb{F}_q^\times}} \frac{Z}{q} = Z \sum_{q \in \mathcal{P}_0} \frac{\phi(q-1)}{q} \geq c_3 Z\sqrt{N}/\log N.$$

Comparing the last two displays, and using the triangle inequality,

$$\sum_{q \in \mathcal{P}_0} \sum_{h \bmod q} \left| Z(q, h) - \frac{Z}{q} \right| \geq \frac{1}{2}c_3 Z\sqrt{N}/\log N.$$

Applying Cauchy–Schwarz (viewing $|Z(q, h) - Z/q| = q^{-1/2} \cdot q^{1/2}|Z(q, h) - Z/q|$),

$$\left(\sum_{q \in \mathcal{P}_0} \sum_{h \bmod q} \left| Z(q, h) - \frac{Z}{q} \right| \right)^2 \leq \#\mathcal{P}_0 \cdot \sum_{q \in \mathcal{P}_0} q \sum_{h \bmod q} \left(Z(q, h) - \frac{Z}{q} \right)^2.$$

Since $\#\mathcal{P}_0 \leq \pi(\sqrt{N})$, we conclude that

$$\sum_{q \in \mathcal{P}_0} q \sum_{h \bmod q} \left(Z(q, h) - \frac{Z}{q} \right)^2 \geq \frac{(\frac{1}{2}c_3 Z\sqrt{N}/\log N)^2}{\pi(\sqrt{N})} \gg Z^2\sqrt{N}/\log N.$$

On the other hand, Proposition 2.4 implies that the left-hand side of the last display is $O(NZ)$. Thus, $\#\mathcal{N} = Z \ll N^{1/2} \log N$.

We have shown what was claimed at the start of this section, with the constant $c_1 = \frac{1}{2}c_3$: For all but $O(N^{1/2} \log N)$ integers $\alpha \in [-N, N]$, we have $\#\mathcal{P}(\alpha) > \frac{1}{2}c_3\sqrt{N}/\log N$.

4.3. **Finding q with $v_q(\alpha^{q-1} - 1) = 1$.** Let $\mathcal{E}$ be the collection of integers $\alpha \in [-N, N]$ such that $v_q(\alpha^{q-1} - 1) > 1$ for all $q \in \mathcal{P}(\alpha)$. To complete the proof of Theorem 1.2, it is enough to show that $\#\mathcal{E} \ll N^{1/2} \log N$.

Let $\mathcal{E}'$ be the subset of $\mathcal{E}$ where we keep only those α with $\#\mathcal{P}(\alpha) > \frac{1}{2}c_3\sqrt{N}/\log N$. From our work in the last section, we need only show $\#\mathcal{E}' \ll N^{1/2} \log N$. In fact, we will show that $\#\mathcal{E}' \ll N^{1/2}$.

For each $\alpha \in \mathcal{E}'$ and each $q \in \mathcal{P}(\alpha)$, put

$$\mathcal{A}_q(\alpha) = \{\alpha + jq : 0 < |j| < q/2\} \cap [-N, N].$$

Let us make a few observations about the sets $\mathcal{A}_q(\alpha)$.

First, $\#\mathcal{A}_q(\alpha) \geq \frac{q-1}{2} > \frac{1}{5}\sqrt{N}$ (for large N). Indeed, if $\alpha > 0$, then $\alpha + jq \in [-N, N]$ whenever $-1 \geq j \geq -q/2$, while if $\alpha < 0$, then $\alpha + jq \in [-N, N]$ when $1 \leq j \leq q/2$.

Second, if we fix $\alpha \in \mathcal{E}'$, then the sets $\mathcal{A}_q(\alpha)$ are disjoint for distinct $q \in \mathcal{P}(\alpha)$. Otherwise, we are led to an equation $\alpha + jq = \alpha + j'q'$ where $q, q' \in \mathcal{P}(\alpha)$, $q \neq q'$. This forces q to divide j', which is impossible since $0 < |j'| < \frac{1}{2}q' \leq \frac{1}{2}\sqrt{N} < q$.

Third, suppose that $q \in \mathcal{P}(\alpha) \cap \mathcal{P}(\alpha')$, where α and α' are distinct elements of $\mathcal{E}'$. Then $\mathcal{A}_q(\alpha)$ and $\mathcal{A}_q(\alpha')$ are disjoint. Otherwise, $\alpha = \alpha' + Jq$ for some integer $J \not\equiv 0 \pmod{q}$. Then

$$\alpha^{q-1} \equiv \alpha'^{q-1} + J(q-1)q\alpha'^{q-2} \pmod{q^2},$$

contradicting that $\alpha^{q-1} \equiv \alpha'^{q-1} \equiv 1 \pmod{q^2}$.

Let $\mathcal{A}(\alpha) = \cup_{q \in \mathcal{P}(\alpha)} \mathcal{A}_q(\alpha)$. By the first and second observations,

$$\sum_{\alpha \in \mathcal{E}'} \#\mathcal{A}(\alpha) = \sum_{\alpha \in \mathcal{E}'} \sum_{q \in \mathcal{P}(\alpha)} \#\mathcal{A}_q(\alpha) \geq \#\mathcal{E}' \cdot \#\mathcal{P}(\alpha) \cdot \frac{1}{5}\sqrt{N} > \#\mathcal{E}' \cdot \frac{1}{10}c_3 \cdot N/\log N.$$

On the other hand, since each $\mathcal{A}(\alpha) \subseteq [-N, N]$, the second and third observations imply that

$$\sum_{\alpha \in \mathcal{E}'} \#\mathcal{A}(\alpha) = \sum_{|n| \leq N} \sum_{\alpha \in \mathcal{E}'} 1_{n \in \mathcal{A}(\alpha)}$$

$$= \sum_{|n| \leq N} \sum_{\alpha \in \mathcal{E}'} \sum_{q \in \mathcal{P}(\alpha)} 1_{n \in \mathcal{A}_q(\alpha)}$$

$$= \sum_{|n| \leq N} \sum_{q \in (\frac{1}{2}\sqrt{N}, \sqrt{N}]} \sum_{\substack{\alpha \in \mathcal{E}' \\ q \in \mathcal{P}(\alpha)}} 1_{n \in \mathcal{A}_q(\alpha)}$$

$$\leq \sum_{|n| \leq N} \sum_{q \in (\frac{1}{2}\sqrt{N}, \sqrt{N}]} 1 \ll N^{3/2}/\log N.$$

(Here the second observation has been used to go from the first line to the second, while the third observation has been used to go from the third line to the fourth.) Comparing the last two displays gives $\#\mathcal{E}' \ll N^{1/2}$, as claimed. This completes the proof of Theorem 1.2.

Remark 4.2. For any *fixed* integer β with $|\beta| > 1$, Hypothesis 4.1 holds for all large N, as a consequence of the Chebotarev density theorem applied to $\mathbb{Q}(\sqrt{\beta})$. (Alternatively, one can

apply the prime number theorem for arithmetic progressions.) Following the above arguments, we conclude that α, β is special for all but $O(N^{1/2} \log N)$ integers α with $|\alpha| \leq N$.

Acknowledgements

References

1. G. Banaszak, *Mod p logarithms* $\log_2 3$ *and* $\log_3 2$ *differ for infinitely many primes*, Ann. Math. Sil. (1998), no. 12, 141–148.
2. E. Bombieri, *On the large sieve*, Mathematika **12** (1965), 201–225.
3. H. Cohen, *Number theory. Vol. I. Tools and Diophantine equations*, Graduate Texts in Mathematics, vol. 239, Springer, New York, 2007.
4. C. Corrales-Rodrigáñez and R. Schoof, *The support problem and its elliptic analogue*, J. Number Theory **64** (1997), 276–290.
5. A. Dunn, B. Kerr, I.E. Shparlinski, and A. Zaharescu, *Bilinear forms in Weyl sums for modular square roots and applications*, Adv. Math. **375** (2020), 107369, 58.
6. P.X. Gallagher, *The large sieve*, Mathematika **14** (1967), 14–20.
7. M. Just and P. Pollack, *Comparing multiplicative orders mod p, as p varies*, New York J. Math. **27** (2021), 600–614.
8. O. Järviniemi, *Equality of orders of a set of integers modulo a prime*, Proc. Amer. Math. Soc. **149** (2021), 3651–3668.
9. A. Schinzel, *On the congruence* $a^x \equiv b$ (mod p), Bull. Acad. Polon. Sci. Sér. Sci. Math. Astronom. Phys. **8** (1960), 307–309.
10. A. Schinzel and J. Wójcik, *On a problem in elementary number theory*, Math. Proc. Cambridge Philos. Soc. **112** (1992), 225–232.

Steklov Institute of Mathematics, 8 Gubkin Street, Moscow, 119991, Russia

Email address: konyagin@mi-ras.ru

Department of Mathematics, University of Georgia, Athens, GA 30602, USA

Email address: pollack@uga.edu