Comparing multiplicative orders mod p, as p varies

Matthew Just and Paul Pollack

ABSTRACT. Schinzel and Wójcik have shown that if α, β are rational numbers not 0 or ± 1, then $\mathrm{ord}_p(\alpha) = \mathrm{ord}_p(\beta)$ for infinitely many primes p, where $\mathrm{ord}_p(\cdot)$ denotes the order in $\mathbb{F}_p^\times$. We begin by asking: When are there infinitely many primes p with $\mathrm{ord}_p(\alpha) > \mathrm{ord}_p(\beta)$? We write down several families of pairs α, β for which we can prove this to be the case. In particular, we show this happens for "100%" of pairs $A, 2$, as A runs through the positive integers. We end on a different note, proving a version of Schinzel and Wójcik's theorem for the integers of an imaginary quadratic field K: If $\alpha, \beta \in \mathscr{O}_K$ are nonzero and neither is a root of unity, then there are infinitely many maximal ideals P of $\mathscr{O}_K$ for which $\mathrm{ord}_P(\alpha) = \mathrm{ord}_P(\beta)$.

CONTENTS

1. Introduction

Let α, β be rational numbers, not 0 or ± 1. For all but finitely many primes p, both α and β are p-adic units, and so it is sensible to talk about their multiplicative orders upon reduction mod p. Schinzel and Wójcik [SW92], extending unpublished investigations of J.S. Wilson, J.G. Thompson, and J.W.S. Cassels, proved that there are infinitely many primes p for which $\mathrm{ord}_p(\alpha) = \mathrm{ord}_p(\beta)$. Equivalently (since $\mathbb{F}_p^\times$ is cyclic), α and β generate the same subgroup of $\mathbb{F}_p^\times$ infinitely often.

2010 *Mathematics Subject Classification.* Primary 11A07, 11R11; Secondary 11A15.
Key words and phrases. multiplicative order, support problem, Schinzel–Wójcik problem, anti-elite prime, anti-elite number, order-dominant pair.

It is an open problem to characterize the triples $\alpha, \beta, \gamma \in \mathbb{Q}^\times \setminus \{\pm 1\}$ for which $\mathrm{ord}_p(\alpha) = \mathrm{ord}_p(\beta) = \mathrm{ord}_p(\gamma)$ infinitely often. But in a recent preprint, Järviniemi presents such a characterization not just for triples, but for tuples of any fixed length, conditional on the Generalized Riemann Hypothesis [Jä20]. (See [PS09] for earlier GRH-conditional results, and [Wój96, Fou18] for related results conditional not on GRH but on Schinzel's "Hypothesis H" [SS58].) Sticking instead to pairs α, β but taking the problem in a different direction, various authors have investigated the distribution of p for which $\mathrm{ord}_p(\alpha) \mid \mathrm{ord}_p(\beta)$ (see [MS00] and [MSS19]).

It is known that if $\alpha, \beta \in \mathbb{Q}^\times \setminus \{\pm 1\}$ and $\mathrm{ord}_p(\alpha) = \mathrm{ord}_p(\beta)$ for all but finitely many primes p, then $\alpha = \beta$ or $\alpha = \beta^{-1}$ (see [Sch70] or [CRnS97]). A natural complement to the theorem of Schinzel and Wójcik would be a characterization of those pairs $\alpha, \beta \in \mathbb{Q}^\times \setminus \{\pm 1\}$ for which

$$\mathrm{ord}_p(\alpha) > \mathrm{ord}_p(\beta) \qquad \text{for infinitely many primes } p. \tag{1}$$

Call the (ordered) pair α, β order-dominant if (1) holds.

Under GRH, we have a completely satisfactory classification of order-dominant pairs. Assume, as above, that $\alpha, \beta \in \mathbb{Q}^\times \setminus \{\pm 1\}$. Then α, β is order-dominant if and only if α is not a power of β.[1] It seems difficult to obtain a result of comparable strength unconditionally. Our first three theorems describe partial progress. Each reports on certain families of integers A, B for which we can prove the order-dominance of A, B without any unproved hypothesis. We mostly (but not exclusively) restrict attention to positive integers A, B; this allows us to illustrate the basic methods while avoiding technical complications. As will become clear shortly, the limitations of our methods manifest already in this restricted situation; given these limitations, we have tried optimize the exposition for clarity rather than generality.

Below, $\left(\frac{\cdot}{\cdot}\right)$ denotes the Legendre–Jacobi–Kronecker symbol.

Theorem 1.

(i) *Let A, B be odd positive integers. Then A, B is order-dominant if either*

$$\left(\frac{-B(1-B)}{A}\right) = -1 \quad \textit{or} \quad \left(\frac{1-B}{A}\right) = -1.$$

(ii) *The pair $2, B$ is order-dominant for every odd positive integer B.*

(iii) *The pair $A, 2$ is order-dominant for every odd positive integer A with $\left(\frac{-1}{A}\right) = -1$ or $\left(\frac{-2}{A}\right) = -1$, i.e., all odd positive $A \not\equiv 1 \pmod 8$.*

(iv) *If A, B are coprime positive integers with $B > A^4$, then $-A, B$ is order-dominant.*

[1] The "only if" half is clear. For the "if" direction: When α, β are multiplicatively independent, Järviniemi [Jä20, Theorem 1.4] proves (under GRH) that $\mathrm{ord}_p(\alpha)/\mathrm{ord}_p(\beta)$ can be made arbitrarily large, which certainly implies the order-dominance of α, β. When α, β are multiplicatively dependent but α is not a power of β, the order-dominance of α, β follows (unconditionally) from an elementary argument with Zsigmondy's theorem.

For example, it follows from Theorem 1 and its proof (see Remark 5(ii)) that if A and B are any of $2, 3, 5$, or 7, and $A \neq B$, then there are infinitely many primes p with $\mathrm{ord}_p(A) > \mathrm{ord}_p(B)$.

When $(A, B) \in \{(2, 3), (3, 2), (2, 5), (5, 2)\}$, Theorem 1 was implicitly proved by Banaszak in [Ban98] (see the proofs of Theorems 1 and 2 in [Ban98]), although his results were not stated this way. Our proofs are essentially the same as his for these cases.

Theorem 1(iii) leaves untouched the pairs $A, 2$ with $A \equiv 1 \pmod 8$. We can show that most such pairs are order-dominant. In fact, we have the following stronger result.

Theorem 2. *The pair $A, 2$ is order-dominant for* almost all *positive integers A, meaning that the set of exceptional A has asymptotic density* 0.

(Note that Theorem 2, unlike Theorem 1(iii), allows A to be even.) The proof of Theorem 2 begins by establishing an explicit (though slightly technical) sufficient condition for $A, 2$ to be order-dominant, involving properties of Fermat numbers. The A for which this condition fails, which we term anti-elite numbers, are then shown to be rare. See Remark 8 for the list of anti-elite A up to 150.

The proofs of Theorems 1 and 2, when they succeed, prove more than the order-dominance of α, β. For all the pairs handled there, what is actually proved is that for infinitely many primes p, the ratio $\mathrm{ord}_p(\alpha)/\mathrm{ord}_p(\beta)$ is a positive even integer. Evenness stems from the fact that the primes p we produce have α not a square modulo p, which we detect by quadratic reciprocity. One might hope to use higher reciprocity laws to generate further examples of order-dominant pairs. Our next theorem, whose proof depends on cubic reciprocity, is a modest step in this direction.

Theorem 3. *Let A be an integer for which $3 \nmid A$ and $A^2 \not\equiv 1 \pmod 9$. For infinitely many primes p, the ratio $\mathrm{ord}_p(A)/\mathrm{ord}_p(-3)$ is an integer multiple of 3. Thus, both $A, -3$ and $A, 3$ are order-dominant.*

(To see the claim about $A, 3$, observe that $\mathrm{ord}_p(3)$ is at most twice $\mathrm{ord}_p(-3)$, and so at most two-thirds of $\mathrm{ord}_p(A)$.) Unfortunately, the proof of Theorem 3 is not very amenable to generalization, although certain other pairs with $B = \pm 3\square$ (i.e., ± 3 times a square) could be treated in a similar fashion. Analogously, the law of biquadratic reciprocity could be used to establish order-dominance of certain pairs A, B with $B = -\square$.

One consequence of Theorem 3 is that the pair $4, 3$ is order-dominant. This could certainly not be proved by the methods of Theorem 1 or 2, since 4 is a square modulo every p.

Theorems 1, 2, and 3 (as well as their methods of proof) still leave us quite far from the GRH-conditional characterization of order dominant pairs. An interesting, difficult-seeming test case is the problem of proving that

$$\mathrm{ord}_p(17) > \mathrm{ord}_p(2) \qquad \text{for infinitely many primes } p.$$

We hope that interested readers will take up this challenge!

Our final theorem is of a quite different nature. We prove the analogue of Schinzel and Wójcik's result for the integers of an imaginary quadratic field.

Theorem 4. *Let K be an imaginary quadratic field with ring of integers $\mathscr{O}_K$. For nonzero $\alpha, \beta \in \mathscr{O}_K$, neither of which is a root of unity, there are infinitely many prime ideals P of $\mathscr{O}_K$ for which α and β generate the same subgroup of $(\mathscr{O}_K/P)^\times$.*

For example, $1+i$ and $2+i$ generate the same subgroup of $(\mathbb{Z}[i]/(\pi))^\times$ for infinitely many Gaussian primes π.

While the proof of Theorem 4 follows the same basic strategy as [SW92], there are essential differences. It is important for us to have available auxiliary primes ℓ for which the ℓth power map, mod ℓ, is induced by a nontrivial automorphism of K. In fact, we will use that all primes $\ell \equiv -1 \pmod{\Delta}$ have this property, where Δ is the discriminant of K; this explains the requirement in the theorem that K is imaginary.

It would be interesting to relax the restriction in Theorem 4 that α and β be integers of the field K. While our method of proof works for many pairs of nonintegral $\alpha, \beta \in K$, an elegant general statement does not seem forthcoming by these arguments.

Notation and conventions. Since $\mathrm{ord}_P(\cdot)$ is being used for the multiplicative order mod P, the P-adic valuation will be denoted $v_P(\cdot)$. We use $\lambda(\cdot)$ for Carmichael's function; that is, $\lambda(n)$ is the exponent of the multiplicative group mod n. We write $\langle g \rangle$ for the cyclic subgroup generated by a group element g.

We say that a statement about positive integers n holds whenever n is sufficiently divisible if there is a positive integer K such that the statement holds for all n divisible by $K!$. Note that if each of two statements holds whenever n is sufficiently divisible, then their conjunction holds for all sufficiently divisible n. One should think of the requirement that n be sufficiently divisible as analogous to the condition, in real analysis, that ϵ be sufficiently close to 0. In fact, this is a bit more than an analogy: Asking that n be sufficiently divisible amounts precisely to asking that n be close enough to 0 in $\hat{\mathbb{Z}}$, the profinite completion of the integers.

The requirement of sufficient divisibility will come up in the following way. We have a commutative ring R, an ideal I for which R/I is finite, and an element $A \in R$ that is invertible modulo I. Then $A^n \equiv 1 \pmod{I}$ whenever n is sufficiently divisible. Of course, it is simple enough here to say that the congruence holds whenever n is divisible by $\#(R/I)^\times$. But later it will be convenient to suppress explicit mention of the required divisibility conditions.

2. First examples of order-dominant pairs: Proof of Theorem 1

Suppose that p is a prime with $\left(\frac{A}{p}\right) = -1$ and that p divides $A^n - B$ for some even positive integer n. Since $B \equiv A^n \equiv (A^{n/2})^2 \pmod{p}$, we see that

- B is in the subgroup generated by A mod p, *and*
- B is a square mod p.

Since A is not a square mod p, it cannot be that A is in the subgroup generated by B mod p. Hence, $\langle B \bmod p \rangle \subsetneq \langle A \bmod p \rangle$, and $\mathrm{ord}_p(A) > \mathrm{ord}_p(B)$. So to prove A, B is order-dominant, it suffices to produce infinitely many primes p of this kind.

Consider the situation where A, B are odd and positive with $\left(\frac{-B(1-B)}{A}\right) = -1$. Then A is coprime to both B and $1-B$. We will locate primes p with $\mathrm{ord}_p(A) > \mathrm{ord}_p(B)$ from among the prime divisors of

$$\frac{A^n - B}{B-1},$$

for suitably chosen positive integers n. Loosely speaking, what we show is that as n gets more and more divisible, our procedure reveals larger and larger primes p with $\mathrm{ord}_p(A) > \mathrm{ord}_p(B)$. (Precisely: As n approaches 0 in $\hat{\mathbb{Z}}$, the discovered prime p approaches ∞ in $\bar{\mathbb{R}} = \mathbb{R} \cup \{\pm\infty\}$.)

If n is sufficiently divisible, then $\frac{A^n-B}{B-1} = \frac{A^n-1}{B-1} - 1 \in \mathbb{Z}^+$, and (since $\gcd(A, 4(B-1)) = 1$) in fact $\frac{A^n-B}{B-1} \equiv -1 \pmod 4$. By quadratic reciprocity (for the Jacobi symbol) and the first supplementary law,

$$\begin{aligned}\left(\frac{A}{(A^n-B)/(B-1)}\right) &= (-1)^{(A-1)/2}\left(\frac{(A^n-B)/(B-1)}{A}\right) \\ &= \left(\frac{-1}{A}\right)\left(\frac{-B(B-1)}{A}\right) = \left(\frac{-B(1-B)}{A}\right) = -1.\end{aligned}$$

Thus, we can choose p dividing $\frac{A^n-B}{B-1}$ with $\left(\frac{A}{p}\right) = -1$. Assuming that n is even (which holds whenever n is sufficiently divisible), we are in the situation described in the first paragraph of this section, and so $\mathrm{ord}_p(A) > \mathrm{ord}_p(B)$.

It remains to see that infinitely many distinct p arise in this construction. For that, it is enough to show that if p is a fixed prime and n is sufficiently divisible, then p does not divide $\frac{A^n-B}{B-1}$. If p divides A, then $p \nmid A^n - B$ for any n, and so $p \nmid \frac{A^n-B}{B-1}$. So suppose $p \nmid A$. If n is sufficiently divisible, $A^n \equiv 1 \pmod{p(B-1)}$ and so $\frac{A^n-B}{B-1} \equiv -1 \pmod p$. Hence, $p \nmid \frac{A^n-B}{B-1}$.

Now suppose that A, B are odd and positive with $\left(\frac{1-B}{A}\right) = -1$. Again, A is coprime to $B-1$. We look at primes dividing expressions of the form

$$\frac{BA^n - 1}{B-1}.$$

If n is sufficiently divisible, then

$$\frac{BA^n-1}{B-1} \in \mathbb{Z}^+, \quad \text{with} \quad \frac{BA^n-1}{B-1} \equiv 1 \pmod 4.$$

Moreover,

$$\left(\frac{A}{(BA^n-1)/(B-1)}\right) = \left(\frac{(BA^n-1)/(B-1)}{A}\right) = \left(\frac{1-B}{A}\right) = -1.$$

Hence, there is a prime divisor p of $(BA^n-1)/(B-1)$ with $\left(\frac{A}{p}\right) = -1$. Assuming n even, $1/B \equiv A^n \equiv (A^{n/2})^2 \bmod p$, and so (reasoning as in the first paragraph of this section) $\langle 1/B \bmod p\rangle \subsetneq \langle A \bmod p\rangle$. Hence, $\mathrm{ord}_p A > \mathrm{ord}_p(1/B) = \mathrm{ord}_p B$. That infinitely many distinct p arise follows from the observation that for any fixed p not dividing A, and all n that are sufficiently divisible, $\frac{BA^n-1}{B-1} \equiv \frac{B-1}{B-1} \equiv 1 \pmod p$.

We turn now to (ii). To handle pairs $2, B$ with B odd and positive, we look at p dividing
$$\frac{4\cdot 2^n - B}{|4-B|}.$$
Whenever n is sufficiently divisible,
$$\frac{4\cdot 2^n - B}{|4-B|} \in \mathbb{Z}^+, \quad \text{and} \quad \frac{4\cdot 2^n - B}{|4-B|} \equiv \pm 3 \pmod 8.$$
Thus, $\left(\frac{2}{(4\cdot 2^n - B)/|4-B|}\right) = -1$. Choose p dividing $\frac{4\cdot 2^n - B}{|4-B|}$ with $\left(\frac{2}{p}\right) = -1$. Then $B \equiv 2^{n+2} \equiv (2^{(n/2+1)})^2 \pmod p$, and so $\langle B \bmod p\rangle \subsetneq \langle 2 \bmod p\rangle$. Hence, $\mathrm{ord}_p(2) > \mathrm{ord}_p(B)$. Infinitely many distinct p arise this way since, for each fixed odd prime p and all n that are sufficiently divisible, $\frac{4\cdot 2^n - B}{|4-B|} \equiv \frac{4-B}{|4-B|} \equiv \pm 1 \pmod p$.

We breeze over the proof of (iii), concerning pairs $A, 2$ with $\left(\frac{-1}{A}\right) = -1$, since the argument parallels the ones already described. This time one looks at primes dividing $2A^n - 1$, with n sufficiently divisible. If $\left(\frac{-1}{A}\right) = 1$ but $\left(\frac{-2}{A}\right) = -1$, one considers prime divisors of $A^n - 2$, with n sufficiently divisible. We leave the details to the reader.

Finally we treat (iv). Let A, B be coprime integers larger than 1 with $B > A^4$. We look at primes dividing
$$\frac{A^{4+n} - B}{B - A^4}.$$
For each prime p,
$$v_p\left(\frac{A^{4+n} - B}{B - A^4} + 1\right) = v_p(A^n - 1) + v_p(A^4) - v_p(B - A^4).$$
If p is fixed and n is sufficiently divisible, then the right-hand side is positive and in fact exceeds $v_p(4A)$: If $p \mid A$, this is clear, since $v_p(B - A^4) = 0$ while $v_p(A^4) > v_p(4A)$. If $p \nmid A$, we use that $v_p(A^n - 1)$ can be made arbitrarily large by making n sufficiently divisible. It follows that $\frac{A^{4+n} - B}{B - A^4}$ is an integer for all sufficiently divisible n and that
$$\frac{A^{4+n} - B}{B - A^4} \equiv -1 \pmod{4A}.$$
Hence, $\left(\frac{-4A}{(A^{4+n} - B)/(B - A^4)}\right) = \left(\frac{-4A}{-1}\right) = -1$. (We have $\left(\frac{-4A}{-1}\right) = -1$ since $-4A$ is an example of a negative discriminant; one reference for this is [MV07, §9.3].) Choose a prime p dividing $\frac{A^{4+n} - B}{B - A^4}$ with $\left(\frac{-4A}{p}\right) = -1$. Since $p \mid (-A)^{4+n} - B$ and $-A$ is not a square mod p, a familiar argument shows that $\mathrm{ord}_p(-A) > \mathrm{ord}_p(B)$. Our above calculation with valuations implies that if p is fixed, then $v_p(\frac{A^{4+n} - B}{B - A^4}) = 0$ for all sufficiently divisible n, and so this construction produces infinitely many different primes.

Remarks 5.

(i) A slight variant of the proof of Theorem 1(iv) establishes the following more general result. Let A, B be integers larger than 1. Let r_0 be a nonnegative integer such that $v_p(A^{r_0}) \geq v_p(B)$ for all primes p dividing A, and let r be an even integer with $r > r_0 + 3$. If $B > A^r$, then $-A, B$ is order-dominant.

Using this result, it is straightforward to show that for each fixed $A > 1$, and almost all positive integers B (in the sense of asymptotic density), the pair $-A, B$ is order-dominant.

(ii) The cases discussed in Theorem 1 were chosen as representative of the basic method, but there are pairs of positive integers not covered by the conditions of Theorem 1 which can be shown order-dominant by this same strategy. One such pair is $3, 7$ (look at primes dividing $\frac{7\cdot 3^n - 1}{2}$), and another is $2, 6$ (look at primes dividing $2^{n+1} - 3$).

3. Almost all pairs $A, 2$ are order-dominant: Proof of Theorem 2

The basic idea for the proof of Theorem 2 is encapsulated in the next lemma. Let $F_n = 2^{2^n} + 1$ (for $n = 0, 1, 2, 3 \dots$), the nth Fermat number. It is well-known that the F_n are pairwise relatively prime and that if p is a prime divisor of F_n, where $n \geq 2$, then $\mathrm{ord}_p(2) = 2^{n+1}$ and $2^{n+2} \mid p - 1$ (see pages 5, 84 of [Rib96]).

Lemma 6. *Suppose A is a positive integer with the property that*

$$\left(\frac{A}{F_n}\right) = -1 \quad \text{for infinitely many positive integers } n.$$

Then $A, 2$ is order-dominant.

Proof. Choose $n \geq 2$ with $\left(\frac{A}{F_n}\right) = -1$. There is a prime p dividing F_n with $\left(\frac{A}{p}\right) = -1$, and for this prime, $A^{(p-1)/2} \equiv -1 \pmod{p}$. Hence, $\mathrm{ord}_p(A)$ divides $p - 1$ but does not divide $\frac{p-1}{2}$, forcing $v_2(\mathrm{ord}_p(A)) = v_2(p-1)$. It follows that

$$\mathrm{ord}_p(A) \geq 2^{v_2(p-1)} \geq 2^{n+2} > 2^{n+1} = \mathrm{ord}_p(2).$$

Since $p > \mathrm{ord}_p(A) \geq 2^{n+2}$, and n can be chosen arbitrarily large, there are infinitely many p with $\mathrm{ord}_p(A) > \mathrm{ord}_p(2)$. $\square$

Primes A *failing* the hypothesis of Lemma 6 appear already in the literature; Müller [Mö7] calls these anti-elite primes. That is, A is anti-elite if $\left(\frac{A}{F_n}\right) = 1$ for all large enough positive integers n. We will call any integer A satisfying this condition an anti-elite integer.

As Müller observed, trivial changes to the proof of Theorem 4 in [KLS02] show that anti-elite primes are sparse within the collection of all primes. Specifically, the count of anti-elite primes not exceeding x is $O(x/(\log x)^{3/2})$, for all $x \geq 2$.[2] In view of Lemma 6, to prove Theorem 2 it is enough to show that only $o(x)$ positive integers $A \leq x$ are anti-elite, as $x \to \infty$. We prove this in the following more precise form.

Theorem 7. *For each $\epsilon > 0$ and all $x > x_0(\epsilon)$, the number of anti-elite $A \in (1, x]$ is $O_\epsilon(x/(\log x)^{1-\epsilon})$.*

[2] A stronger upper bound of $O(x/(\log x)^2)$ is claimed in [KLS02]. Just [Jus20] points out a small error in the proof and notes that, when corrected, 2 must be replaced by $3/2$. In fact, one can recover an estimate almost as strong as originally claimed by a modification of the proof; see the end of our §3.

Proof. Write $A = A_0 A_1$, where A_1 is the largest odd divisor of A. We will assume that $v_2(\lambda(A_1)) < T - 2$, where

$$T := \left\lfloor \frac{\log(\log x/\log\log x)}{\log 2} \right\rfloor.$$

If $v_2(\lambda(A_1)) \ge T - 2$, then there is a prime p dividing A with $p \equiv 1 \pmod{2^{T-2}}$, and the number of such $A \le x$ is

$$\ll x \sum_{\substack{p \le x \\ p \equiv 1 \pmod{2^{T-2}}}} \frac{1}{p} \ll x \frac{\log\log x}{2^{T-2}} \ll \frac{x(\log\log x)^2}{\log x},$$

which is $O_\epsilon(x/(\log x)^{1-\epsilon})$. Here the sum on p has been estimated by the Brun–Titchmarsh inequality [MV07, Theorem 3.9, p. 90] and partial summation.

We fix a nonnegative integer $t < T - 2$ and count the number of anti-elite $A \in (1, x]$ with $v_2(\lambda(A_1)) = t$. For each such A, the sequence $\{\left(\frac{A}{F_n}\right)\}_{n \ge t+2}$ is purely periodic. Indeed, if $n \ge t + 2$, then $n \ge 2$, so that $F_n \equiv 1 \pmod 8$ and $\left(\frac{2}{F_n}\right) = 1$. Hence, $\left(\frac{A}{F_n}\right) = \left(\frac{A_1}{F_n}\right) = \left(\frac{F_n}{A_1}\right)$, which depends only on F_n modulo A_1. In turn, $F_n = 2^{2^n} + 1 \bmod A_1$ depends only on 2^n modulo $\lambda(A_1)$. Write

$$\lambda(A_1) = 2^{v_2(\lambda(A_1))} B,$$

where B is odd. Since $n \ge t = v_2(\lambda(A_1))$, the residue class of $2^n \bmod \lambda(A_1)$ is determined by 2^n modulo B, which depends only on n modulo $\lambda(B)$. Collecting our results, we see that $\{\left(\frac{A}{F_n}\right)\}_{n \ge t+2}$ is purely periodic (with period dividing $\lambda(B)$).

Since A is anti-elite, it must be that each F_n with $n \ge t + 2$ satisfies $\left(\frac{A}{F_n}\right) = 1$. In particular,

$$\left(\frac{A}{F_n}\right) = 1 \quad \text{for all } n \text{ with} \quad t + 2 \le n < T. \tag{2}$$

Factor $A = ps$, where p is prime, $p \equiv 1 \pmod{2^t}$. Our argument to bound the number of remaining A assumes two different forms according to the sizes of p and s.

Suppose first that $s \le \sqrt{x}$, so that $x/s \ge \sqrt{x}$. It follows from (2) that p, s are prime to $\prod_{t+2 \le n < T} F_n$, and that

$$\left(\frac{p}{F_n}\right) = \left(\frac{s}{F_n}\right) \quad \text{whenever} \quad t + 2 \le n < T. \tag{3}$$

We view s as fixed and count the number of corresponding p. Let $F = \prod_{t+2 \le n < T} F_n$. Keeping in mind that $p \equiv 1 \pmod{2^t}$, we deduce from (3) that p belongs to one of $\prod_{t+2 \le n < T}(\frac{1}{2}\phi(F_n)) = 2^{t-T+2}\phi(F)$ coprime residue classes modulo $2^t F$. (We use here that each symbol $\left(\frac{\cdot}{F_n}\right)$ is a nontrivial quadratic character mod F_n, since F_n is not a square.) Notice that

$$F < \prod_{n=0}^{T-1} F_n = F_T - 2 < F_T.$$

So by our choice of T, and the inequality $t < T-2$, we have $2^t F < 2^t F_T = x^{o(1)}$ (as $x \to \infty$). Since $p = A/s \le x/s$, the Brun–Titchmarsh inequality tells us that the number of possibilities for p is $O(2^{-T}\frac{x}{s\log x})$. Summing on $s \le \sqrt{x}$ shows that the number of possible A in this case is

$$\ll \frac{x}{2^T} \ll \frac{x\log\log x}{\log x}.$$

Now suppose that $s > \sqrt{x}$. Then $p \le x/s < \sqrt{x}$. From (2), we have with $m = A$ that

$$\frac{1}{2^{T-t-2}} \prod_{t+2\le n<T} \left(1 + \left(\frac{m}{F_n}\right)\right) = 1.$$

Since the above left-hand side is nonnegative for every m, we conclude that an upper bound for the count of remaining A is

$$\frac{1}{2^{T-t-2}} \sum_{\substack{p\le\sqrt{x} \\ p\equiv 1 \pmod{2^t}}} \sum_{s\le x/p} \prod_{t+2\le n<T} \left(1 + \left(\frac{sp}{F_n}\right)\right).$$

Expanding the product and bringing the sums on s, p inside gives a main term of size

$$\frac{1}{2^{T-t-2}} \sum_{\substack{p\le\sqrt{x} \\ p\equiv 1 \pmod{2^t}}} \sum_{s\le x/p} 1 \ll \frac{1}{2^{T-t}} x \sum_{\substack{p\le\sqrt{x} \\ p\equiv 1 \pmod{2^t}}} \frac{1}{p} \ll \frac{x\log\log x}{2^T} \ll \frac{x(\log\log x)^2}{\log x}.$$

There are also $2^{T-t-2}-1$ error terms of the form $\frac{1}{2^{T-t-2}}\sum_{p,s}\left(\frac{ps}{D}\right)$, where D is the product of some nonempty subset of $\{F_{t+2}, F_{t+3}, \dots, F_{T-1}\}$. Since Fermat numbers are pairwise coprime, D is not a square, and $\left(\frac{\cdot}{D}\right)$ is a nontrivial Dirichlet character modulo D. Moreover, $D \le F = x^{o(1)}$. Using the trivial bound of D for a nontrivial character sum mod D, we see that

$$\begin{aligned} \sum_{\substack{p\le\sqrt{x} \\ p\equiv 1 \pmod{2^t}}} \sum_{s\le x/p} \left(\frac{ps}{D}\right) &= \sum_{\substack{p\le\sqrt{x} \\ p\equiv 1 \pmod{2^t}}} \left(\frac{p}{D}\right) \sum_{s\le x/p} \left(\frac{s}{D}\right) \\ &\ll D \sum_{\substack{p\le\sqrt{x} \\ p\equiv 1 \pmod{2^t}}} 1 \ll Dx^{1/2}. \end{aligned}$$

Hence, the errors contribute $\ll Dx^{1/2} \ll x^{2/3}$. This is negligible compared to our main term, and so the number of A that arise in this second case is $O(x(\log\log x)^2/\log x)$.

Assembling our results, we have proved that for each t, the number of corresponding A is $O(x(\log\log x)^2/\log x)$. It remains to sum on t. But there are only $O(\log\log x)$ possible values of t, and so the total number of anti-elite $A \le x$ is $O(x(\log\log x)^3/\log x)$, which is $O_\epsilon(x/(\log x)^{1-\epsilon})$. $\square$

Remark 8. The anti-elite numbers up to 150 are

$$1, \mathbf{2}, 4, 8, 9, \mathbf{13}, 15, 16, \mathbf{17}, 18, 21, 25, 26, 30, 32, 34, 35, 36, 42, 49, 50, 52, 60,$$
$$64, 68, 70, 72, 81, 84, \mathbf{97}, 98, 100, 104, 117, 120, 121, 123, 128, 135, 136, 140, 144.$$

Anti-elite primes are shown in bold.

The proof of Theorem 7 is a more careful variant of the proof of Theorem 4 in [KLS02], the primary difference being that we keep track of the exact value of t (the original argument only tracked whether t was small or large, in a certain sense). Inserting this idea back into [KLS02] will show that the count of elite primes up to x is $O_\epsilon(x/(\log x)^{2-\epsilon})$, essentially recovering the bound of $O(x/(\log x)^2)$ claimed in [KLS02]. Under GRH, the first author showed in [Jus20] that the count of elite primes up to x is $O_\epsilon(x^{5/6+\epsilon})$; the present method allows us to replace $5/6$ by $3/4$.

4. Order-dominant pairs $A, -3$ and $A, 3$: Proof of Theorem 3

Let $\zeta = e^{2\pi i/3} = \frac{-1+\sqrt{-3}}{2}$. Below, we work in the ring $\mathbb{Z}[\zeta] = \mathscr{O}_K$, where $K = \mathbb{Q}(\zeta)$. Let $\lambda = 1 - \zeta$, so that $\lambda^2 = -3\zeta$ and the ideal $(\lambda^2) = (3)$.

Take first the case when A is even. Thinking of n as sufficiently divisible (and in particular, even), we set

$$\beta := A^{n/2} - \sqrt{-3}$$

and we attempt to evaluate the cubic residue symbol $\left(\frac{A}{\beta}\right)_3$. Since $\sqrt{-3} = 2\zeta + 1$, we have

$$\beta = A^{n/2} - 1 - 2\zeta. \tag{4}$$

Since $3 \nmid A$, for sufficiently divisible n we find that $A^{n/2} \equiv 1 \pmod 3$, so that

$$\beta \equiv -2\zeta \pmod{\lambda^2}.$$

Hence, $\zeta^2\beta$ is congruent, modulo λ^2, to a rational integer coprime to 3; that is, $\zeta^2\beta$ is primary in the sense required for an application of Eisenstein's ℓth power reciprocity law with $\ell = 3$ (see, e.g., pp. 206–207 of [IR90]). By that law, we deduce that (for sufficiently divisible n)

$$\left(\frac{A}{\beta}\right)_3 = \left(\frac{A}{\zeta^2\beta}\right)_3 = \left(\frac{\zeta^2\beta}{A}\right)_3 = \left(\frac{-\zeta^2\sqrt{-3}}{A}\right),$$

so that

$$\left(\frac{A}{\beta}\right)_3^2 = \left(\frac{-3\zeta}{A}\right)_3 = \left(\frac{\lambda^2}{A}\right)_3 = \left(\frac{\lambda}{A}\right)_3^2,$$

forcing $\left(\frac{A}{\beta}\right)_3 = \left(\frac{\lambda}{A}\right)_3$, since $\left(\frac{A}{\beta}\right)_3$ and $\left(\frac{\lambda}{A}\right)_3$ are third roots of unity. From the supplementary laws for Eisenstein reciprocity (see p. 365 of [Lem00]),

$$\left(\frac{\lambda}{A}\right)_3 = \left(\frac{\zeta}{A}\right)_3^{\frac{1}{2}(3-1)} = \left(\frac{\zeta}{A}\right)_3 = \zeta^{(A^2-1)/3}.$$

Since $A^2 \not\equiv 1 \pmod 9$, the exponent on ζ is not a multiple of 3. Thus, $\left(\frac{A}{\beta}\right)_3 \neq 1$. In particular, A is not a cube modulo β, in $\mathbb{Z}[\zeta]$.

Since A is even, we see from (4) that when β is written as a $\mathbb{Z}$-linear combination of $1, \zeta$, the coefficient of 1 and the coefficient of ζ are relatively prime. For any β of this kind, a straightforward calculation shows that the canonical map $\mathbb{Z} \to \mathbb{Z}[\zeta]/(\beta)$ is surjective, and so induces an isomorphism $\mathbb{Z}/(N\beta) \cong \mathbb{Z}[\zeta]/(\beta)$. Thus, the calculation of the last paragraph implies that A is not a cube modulo $N\beta = A^n + 3$, in $\mathbb{Z}$. If A were a cube modulo every prime factor of $A^n + 3$, then A would be a cube modulo $A^n + 3$, by Hensel's lemma and the Chinese remainder theorem. (We use here that A is prime to $A^n + 3$, and that $3 \nmid A^n + 3$.) So we can choose a prime p dividing $A^n + 3$ with A not a cube modulo p.

If n is sufficiently divisible, then $3 \mid n$. Then $A^n \equiv -3 \pmod p$ implies that -3 is a cube modulo p and that -3 mod p belongs to the subgroup generated by A mod p. Since A is not a cube mod p, we see A is not in the subgroup generated by -3, and thus $\langle -3 \bmod p \rangle \subsetneq \langle A \bmod p \rangle$. It follows that $\mathrm{ord}_p(A)/\mathrm{ord}_p(-3)$ is an integer larger than 1. To see that this integer is a multiple of 3, notice that $p \equiv 1 \pmod 3$ (otherwise, A would be a cube mod p), that $v_3(\mathrm{ord}_p(A)) = v_3(p-1)$ (since A is a not a cube) and that $v_3(\mathrm{ord}_p(-3)) < v_3(p-1)$ (since -3 is a cube). Thus, $v_3(\mathrm{ord}_p(A)/\mathrm{ord}_p(3)) \geq 1$.

We have shown so far that if n is sufficiently divisible, one can find a prime factor of $A^n + 3$ with $\mathrm{ord}_p(A)/\mathrm{ord}_p(3)$ an integer multiple of 3. To see that infinitely many distinct primes arise, notice that all of the p produced by this construction are odd and coprime to A. Then observe that if p is any fixed prime not dividing $2A$, then $A^n + 3 \equiv 4 \not\equiv 0 \pmod p$ whenever n is sufficiently divisible.

The proof is essentially the same when A is odd, except that now one should set $\beta := \frac{1}{2}(A^{n/2} - \sqrt{-3})$. It is also useful to observe that $\left(\frac{2}{A}\right)_3 = \left(\frac{A}{2}\right)_3 = \left(\frac{1}{2}\right)_3 = 1$. We leave the details to the reader.

5. Equal orders in imaginary quadratic rings: Proof of Theorem 4

Let K be a quadratic field of discriminant $\Delta < 0$, and let α, β be distinct nonzero elements of $\mathscr{O}_K$, neither of which is a root of unity. Let I be the largest ideal divisor of $(\beta - \alpha)$ coprime to (α). The prime ideals P referred to in the conclusion of Theorem 4 will come to us as divisors of the (ideal) expression

$$(\beta\alpha^\ell - 1)/I,$$

where ℓ is a prime number for which $\ell + 1$ is sufficiently divisible. It is important to note that any "sufficiently divisible" hypothesis on $\ell + 1$ is always satisfied by infinitely many primes ℓ; this follows, e.g., from Dirichlet's theorem on primes in progressions. (For an elementary proof of the -1 mod M case of Dirichlet's theorem used here, see §50 of [Nag51].)

If $\ell + 1$ is sufficiently divisible, then $\alpha^{\ell+1} \equiv 1 \pmod I$, so that $\alpha(\beta\alpha^\ell - 1) \equiv \beta - \alpha \equiv 0 \pmod I$. Hence, $(\beta\alpha^\ell - 1)/I$ is a nonzero, integral ideal of $\mathscr{O}_K$. Since $\Delta \mid \ell + 1$ when $\ell + 1$ is sufficiently divisible,

$$\sqrt{\Delta}^\ell \equiv \Delta^{(\ell-1)/2}\sqrt{\Delta} \equiv \left(\frac{\Delta}{\ell}\right)\sqrt{\Delta} \equiv \left(\frac{\Delta}{-1}\right)\sqrt{\Delta} \equiv -\sqrt{\Delta} \pmod{\ell}.$$

So using a bar for complex conjugation (identified with the nontrivial automorphism of K), $\alpha^\ell \equiv \bar{\alpha} \pmod{\ell}$, and

$$\begin{aligned} N((\beta\alpha^\ell - 1)/I) &= N(\beta\alpha^\ell - 1)/N(I) \\ &\equiv N(\beta\bar{\alpha} - 1)/N(I) \pmod{\ell}. \end{aligned}$$

In the last line, division by $N(I)$ mod ℓ is to be understood as multiplication by the inverse of $N(I)$ mod ℓ. The rational number $N(\beta\bar{\alpha}-1)/N(I)$ exceeds 1, since

$$\begin{aligned} N(\beta\bar{\alpha} - 1) - N(I) &\geq N(\beta\bar{\alpha} - 1) - N(\beta - \alpha) \\ &= (\beta\bar{\alpha} - 1)(\bar{\beta}\alpha - 1) - (\beta - \alpha)(\bar{\beta} - \bar{\alpha}) \\ &= (\beta\bar{\beta} - 1)(\alpha\bar{\alpha} - 1) = (N\alpha - 1)(N\beta - 1) > 0. \end{aligned}$$

It follows that if $\ell + 1$ is sufficiently divisible,

$$N(\beta\bar{\alpha} - 1)/N(I) \not\equiv 1 \pmod{\ell}.$$

Thus, there must be a prime ideal P of $\mathscr{O}_K$ dividing $(\beta\alpha^\ell - 1)/I$ with $N(P) \not\equiv 1 \pmod{\ell}$, i.e., with $\ell \nmid (\mathscr{O}_K/P)^\times$. Since $\beta\alpha^\ell \equiv 1 \mod I$, we deduce that $\langle \beta \bmod P\rangle = \langle \alpha^{-\ell} \bmod P\rangle = \langle \alpha \bmod P\rangle$.

To show that infinitely many such P arise, we show that any fixed P is coprime to $(\beta\alpha^\ell - 1)/I$ for all ℓ with $\ell + 1$ sufficiently divisible. This is clear if $P \mid (\alpha)$. Otherwise, choose k for which $P^k \parallel (\beta - \alpha)$. Then $P^k \parallel I$. Whenever $\ell + 1$ is sufficiently divisible,

$$\alpha(\beta\alpha^\ell - 1) \equiv (\beta - \alpha) \pmod{P^{k+1}},$$

which implies that $P^k \parallel (\beta\alpha^\ell - 1)$. But then $P \nmid (\beta\alpha^\ell - 1)/I$.

Remark 9. It would seem interesting to consider the problems of this paper for other algebraic groups. For instance, fix an elliptic curve E over $\mathbb{Q}$ of positive rank, and suppose that $P, Q \in E(\mathbb{Q})$ are points of infinite order. Under what conditions on P, Q are there infinitely many primes p (a) for which P and Q have the same order in $E(\mathbb{F}_p)$? (b) for which the order of P in $E(\mathbb{F}_p)$ is larger than the order of Q?

Acknowledgements

The first author (M.J.) was supported by the UGA Algebraic Geometry, Algebra, and Number Theory RTG grant, NSF award DMS-1344994. The second author (P.P.) was supported by NSF award DMS-2001581. We thank Michael Filaseta, Pieter Moree, Carl Pomerance, Enrique Treviño, and the referee for helpful comments. We are also grateful to MathOverflow user `Hhhhhhhhhhh` for the post which brought this question to our attention [Hhh20].

References

[Ban98] Banaszak, G. Mod p logarithms $\log_2 3$ and $\log_3 2$ differ for infinitely many primes. *Ann. Math. Sil.* (1998), no. 12, 141–148. MR1673013 (2000f:11004), Zbl 0923.11006.

[CRnS97] Corrales-Rodrigáñez, C.; Schoof, R. The support problem and its elliptic analogue. *J. Number Theory* **64** (1997) 276–290. MR1453213 (98c:11049), Zbl 0922.11086.

[Fou18] Fouad, M. On Schinzel–Wójcik problem. Ph.D. thesis, Roma Tre University, 2018.

[Hhh20] Hhhhhhhhhhh. Does there exist a prime p such that $\frac{\mathrm{ord}_p(a)}{\mathrm{ord}_p(b)} > 1$? MathOverflow (2020). URL: `https://mathoverflow.net/q/376093` (version: 2020-11-10).

[IR90] Ireland, K.; Rosen, M. A classical introduction to modern number theory. Second edition. Graduate Texts in Mathematics, 84. *Springer-Verlag, New York*, 1990. MR0661047 (83g:12001), Zbl 0712.11001.

[Jä20] Järviniemi, O. Equality of orders of a set of integers modulo a prime. `arXiv:1912.02554v2 [math.NT]` (2020).

[Jus20] Just, M. On upper bounds for the count of elite primes. *Integers* **20** (2020), no. A76, 5 pages. MR4153076, Zbl 07306622.

[KLS02] Křížek, M.; Luca, F.; Somer, L. On the convergence of series of reciprocals of primes related to the Fermat numbers. *J. Number Theory* **97** (2002) 95–112. MR1939138 (2003i:11015), Zbl 1026.11011.

[Lem00] Lemmermeyer, F. Reciprocity laws. Springer Monographs in Mathematics. *Springer-Verlag, Berlin*, 2000. MR1761696 (2001i:11009), Zbl 0949.11002.

[Mö07] Müller, T. On anti-elite prime numbers. *J. Integer Seq.* **10** (2007), no. 9, 10 pages. MR2346093 (2009e:11012), Zbl 1144.11005.

[MS00] Moree, P.; Stevenhagen, P. A two-variable Artin conjecture. *J. Number Theory* **85** (2000) 291–304. MR1802718 (2001k:11188), Zbl 0966.11042.

[MSS19] Murty, M.R.; Séguin, F.; Stewart, C.L. A lower bound for the two-variable Artin conjecture and prime divisors of recurrence sequences. *J. Number Theory* **194** (2019) 8–29. MR1802718 (2001k:11188), Zbl 1437.11141.

[MV07] Montgomery, H.L.; Vaughan, R.C. Multiplicative number theory. I. Classical theory. Cambridge Studies in Advanced Mathematics, 97. *Cambridge University Press, Cambridge*, 2007. MR2378655 (2009b:11001), Zbl 1245.11002.

[Nag51] Nagell, T. Introduction to number theory. *John Wiley & Sons, Inc., New York; Almqvist & Wiksell, Stockholm*, 1951. MR0043111 (13,207b), Zbl 0042.26702.

[PS09] Pappalardi, F.; Susa, A. On a problem of Schinzel and Wójcik involving equalities between multiplicative orders. *Math. Proc. Cambridge Philos. Soc.* **146** (2009) 303–319. MR2475969 (2010a:11196), Zbl 1242.11070.

[Rib96] Ribenboim, P. The new book of prime number records. Third edition. *Springer-Verlag, New York*, 1996. MR1377060 (96k:11112), Zbl 0856.11001.

[Sch70] Schinzel, A. A refinement of a theorem of Gerst on power residues. *Acta Arith.* **17** (1970) 161–168. MR0284417 (44 #1644), Zbl 0233.10003.

[SS58] Schinzel, A.; Sierpiński, W. Sur certaines hypothèses concernant les nombres premiers. *Acta Arith.* **4** (1958) 185–208; erratum in **5** (1958) 259. MR0106202 (21 #4936), Zbl 0082.25802.

[SW92] Schinzel, A.; Wójcik, J. On a problem in elementary number theory. *Math. Proc. Cambridge Philos. Soc.* **112** (1992) 225–232. MR1171159 (93e:11006), Zbl 0770.11001.

[Wój96] Wójcik, J. On a problem in algebraic number theory. *Math. Proc. Cambridge Philos. Soc.* **119** (1996) 191–200. MR1357038 (97c:11097), Zbl 0854.11051.

Department of Mathematics, University of Georgia, Athens, GA 30602
`justmatt@uga.edu`
`pollack@uga.edu`