# TWO VARIANTS OF A THEOREM OF SCHINZEL AND WÓJCIK ON MULTIPLICATIVE ORDERS

PAUL POLLACK

Abstract. Schinzel and Wójcik have shown that if $\alpha, \beta \in \mathbb{Q}^\times \setminus \{\pm 1\}$, then there are infinitely many primes $p$ where $v_p(\alpha) = v_p(\beta) = 0$ and where $\alpha, \beta$ share the same multiplicative order modulo $p$. We present two variants of their result. First, we give a short and simple proof of the analogous statement where $\mathbb{Q}$ is replaced by any global function field $K$. Second, we show that a similar conclusion holds in the number field case provided one can find a suitable 'auxiliary prime'. Given $K$, $\alpha$, and $\beta$, it appears simple in practice to find such a prime. As an application, we prove there are infinitely many primes $p$ with the same rank of appearance in the sequences of Pell and Fibonacci numbers.

## 1. Introduction

In [SW92], Schinzel and Wójcik showed that whenever $\alpha, \beta \in \mathbb{Q}^\times \setminus \{\pm 1\}$, there are infinitely many primes $p$ where the $p$-adic valuations $v_p(\alpha) = v_p(\beta) = 0$ and where $\alpha$ and $\beta$ share the same multiplicative order when reduced modulo $p$. They aptly titled their paper *On a problem in elementary number theory*. It is natural to wonder whether analogous theorems hold if the problem is transferred from elementary to algebraic number theory.

Number field generalizations were taken up by Wójcik in [W96]. There Wójcik works under the assumption of Schinzel's unproved 'Hypothesis H' (introduced in [SS58]) concerning simultaneous prime values of integer-coefficient polynomials. Variants of the Schinzel–Wójcik theorem obtained without extra hypotheses are almost entirely absent from the literature. The exception that proves the rule: In [JP21] a version of the Schinzel–Wójcik theorem is demonstrated for imaginary quadratic fields $K$. Unfortunately the statement there requires $\alpha$ and $\beta$ to belong to the ring of integers of $K$; handling general $\alpha, \beta \in K^\times$ (satisfying the natural condition that neither be a root of unity) would seem to require a new idea.

In this note we present two unconditional variants of the Schinzel–Wójcik theorem. The first is a version for an arbitrary global function field.

2020 *Mathematics Subject Classification.* Primary 11R44; Secondary 11A07, 11R04.

*Key words and phrases.* Schinzel–Wójcik problem, multiplicative order, global field, Artin's primitive root conjecture, rank of appearance.

**Theorem 1.1.** *Let $K$ be an algebraic function field over the finite field $F$. Assume $F$ is the full field of constants of $K$. For every $\alpha, \beta \in K \setminus F$, there are infinitely many places $P$ of $K$ for which $v_P(\alpha) = v_P(\beta) = 0$ and where $\alpha, \beta$ share the same multiplicative order in the residue field $\mathcal{O}_P/P$.*

(When discussing function fields we set up our definitions following Stichenoth's monograph [Sti09]; in particular, $P$ is equal to, not merely identifiable with, the maximal ideal of $\mathcal{O}_P$.) Our proof of Theorem 1.1 is similar in spirit to the argument of [SW92]. However, it is both shorter and simpler; that all the residue fields of $K$ have the same positive characteristic is a great help.

One should be able to derive results significantly stronger than Theorem 1.1 by applying methods used to investigate Artin's primitive root conjecture. Over $\mathbb{Q}$ Järviniemi [JÖ21] has characterized, conditional on the Generalized Riemann Hypothesis (GRH), those tuples of nonzero rational numbers $a_1, \dots, a_t$ for which there are infinitely many primes $p$ with $a_1, \dots, a_t$ sharing the same multiplicative order modulo $p$. (See [PS09] for earlier GRH-conditional investigations.) For example, Järviniemi shows this conclusion holds whenever $a_1, \dots, a_t > 1$. (This last statement also follows from Hypothesis H as earlier demonstrated by Wójcik [WÓ96].) Related GRH-conditional results for general number fields are contained in recent work of Järviniemi and Perucca [JP23]. When such problems are studied in the function field setting, usually GRH can be substituted with the Riemann Hypothesis for curves (see for instance [PS95] and [Ros02, Chapter 10]). As the Riemann Hypothesis for curves is a theorem of Weil (see [Sti09, Chapter 5] for a relatively elementary proof), one expects that results of this same kind could be established unconditionally. Needless to say, such arguments when fully unwound would be substantially more intricate than what we offer for Theorem 1.1.

Our second theorem concerns the number field case. Here we show that the conclusion of the Schinzel–Wójcik theorem holds for a given $K, \alpha$, and $\beta$ provided one can locate an auxiliary prime satisfying appropriate conditions. This auxiliary prime strategy (but with a different requirement on the prime) is already present in the original proof of Schinzel and Wójcik; happily, in the setting of [SW92], those authors could show that the sought-after prime always exists! So far we have not been so lucky.

If $K$ is a number field and $\alpha, \beta \in K^\times$, we call a nonzero prime ideal $P$ of $\mathcal{O}_K$ generous with respect to $K, \alpha, \beta$ if

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

(ii) $\alpha$ and $\beta$ generate topologically the same subgroup of $K_P^\times$, where $K_P$ is the $P$-adic completion of $K$. Equivalently but more concretely: For each nonnegative integer $k$, there are integers $n$ and $m$ with

$$\alpha^n \equiv \beta \pmod{P^k} \quad \text{and} \quad \beta^m \equiv \alpha \pmod{P^k}.$$

Here and below, where congruences appear relating elements not assumed to lie in $\mathcal{O}_K$, the congruences are to be understood as holding in the localization $\mathcal{O}_P$.

**Theorem 1.2.** *Let $K$ be a number field and let $\alpha, \beta \in K^\times$. Suppose there is a nonzero prime ideal $P_0$ of $\mathcal{O}_K$ that is generous with respect to $K, \alpha, \beta$. Then there are infinitely many nonzero prime ideals $P$ of $\mathcal{O}_K$ for which $v_P(\alpha) = v_P(\beta) = 0$ and where $\alpha, \beta$ have the same multiplicative order in $\mathcal{O}_P/P\mathcal{O}_P$.*

Our proof of Theorem 1.2 borrows essential ideas from [SW92] but the argument is complicated by the need in several places to work with ideals rather than elements. It may be that generous primes always exist if $\alpha, \beta \in K^\times$ and neither is a root of unity. We do not know how to prove this speculation or any reasonable approximation to such a statement. However, in practice it seems easy to find a generous prime given $K, \alpha$ and $\beta$. We illustrate this with an example at the end of §3 which has a consequence of independent interest: There are infinitely many primes whose rank of appearance (see §3 for the definition) is the same in the sequence of Pell numbers and the sequence of Fibonacci numbers.

## 2. Schinzel–Wójcik for function fields: Proof of Theorem 1.1

In what follows we let $p$ denote the characteristic of $K$. We write $\mathbb{P}_K$ for the set of places of $K/F$. Writing $\mathrm{multord}_P$ for the multiplicative order in $\mathcal{O}_P/P$, let

$$\begin{aligned}\mathcal{S} &= \mathcal{S}_K(\alpha, \beta) \\ &= \{P \in \mathbb{P}_K : v_P(\alpha) = v_P(\beta) = 0 \text{ and } \mathrm{multord}_P(\alpha) = \mathrm{multord}_P(\beta)\}.\end{aligned}$$

The proof of Theorem 1.1 is based on the following simple but fundamental observation: Suppose $v_P(\alpha) = v_P(\beta) = 0$ while $v_P(\alpha\beta^{p^m} - 1) > 0$ for a certain nonnegative integer $m$. Then $\beta^{p^m} = \alpha^{-1}$ in $\mathcal{O}_P/P$. Since the $p$th power map is an automorphism of $\mathcal{O}_P/P$, we conclude that

$$\begin{aligned}\mathrm{multord}_P(\beta) = \mathrm{multord}_P(\beta^p) = \ldots &= \mathrm{multord}_P(\beta^{p^m}) \\ &= \mathrm{multord}_P(\alpha^{-1}) = \mathrm{multord}_P(\alpha).\end{aligned}$$

Thus, $P \in \mathcal{S}$. (Compare with the 'Proposition' on p. 225 of [SW92].)

We now suppose for a contradiction that $\#\mathcal{S} < \infty$. For each $P \in \mathcal{S}$, write $\#\mathcal{O}_P/P = p^{f_P}$, and put $f = \mathrm{lcm}_{P\in\mathcal{S}}[f_P]$.

Since $\beta \notin F$, we have that $\beta$ is transcendental over $F$, and so there is at most one positive integer $m$ with $\alpha\beta^{p^m} - 1 = 0$. So for all sufficiently large positive integers $n$, say all $n \geq n_0$,

$$x_n := \frac{\alpha\beta^{p^{(n+1)f}} - 1}{\alpha\beta^{p^{nf}} - 1} \in K^\times. \tag{2.1}$$

Let $P$ be a place of $K$ for which $v_P(\alpha) = v_P(\beta) = 0$. If $P$ appears in the support of $(x_n)$ for at least one $n \geq n_0$, then $P \in \mathcal{S}$. Let us argue that each fixed $P \in \mathcal{S}$ appears in the support of $x_n$ for only finitely many $n$. We start by observing that

$$\beta^{p^{(n+1)f}} - \beta^{p^{nf}} = \beta^{p^{nf}}(\beta^{p^{nf}(p^f-1)} - 1).$$

For each fixed positive integer $m$ and all $n \geq m$,

$$\#(\mathcal{O}_P/P^m)^\times = p^{f_P(m-1)}(p^{f_P} - 1) \quad \text{divides} \quad p^{nf}(p^f - 1),$$

so that $v_P(\beta^{p^{(n+1)f}} - \beta^{p^{nf}}) \geq m$. It follows now from the ultrametric inequality that $\{\beta^{p^{nf}}\}$ is a Cauchy sequence in the $P$-adic topology. Thus, writing $K_P$ for the $P$-adic completion of $K$, we have that $\beta^{p^{nf}} \to \hat{\beta}$ for some $\hat{\beta} \in K_P$. The numerator and denominator in (2.1) both tend to $\alpha\hat{\beta} - 1$, which is nonzero (otherwise $\alpha = 1/\hat{\beta}$ satisfies $\alpha^{p^f} = 1/\hat{\beta}^{p^f} = 1/\hat{\beta} = \alpha$, forcing $\alpha \in F$). Hence, $x_n \to 1$ in $K_P$, implying $v_P(x_n) = 0$ for all large enough $n$.

We are supposing $\mathcal{S}$ is finite. Thus, the argument of the last paragraph implies that for all large $n$, every place in the support of $x_n$ is one of the finitely many places belonging to the union of the supports of $\alpha$ and $\beta$. Fix a place $P$ in the support of $\alpha$ or $\beta$. If $v_P(\beta) < 0$, the strong triangle inequality implies that $v_P(x_n) = (p^{(n+1)f} - p^{nf})v_P(\beta) < 0$ for all large values of $n$ while if $v_P(\beta) \geq 0$ then $v_P(x_n) = 0$ for all large $n$. (To see this it is helpful to take cases according to whether $v_P(\alpha) < 0$, $v_P(\alpha) = 0$, or $v_P(\alpha) > 0$.)

Hence, once $n$ is large enough there are no places $P$ with $v_P(x_n) > 0$. That is, $x_n$ has no zeros. As principal divisors have degree 0 (see [Sti09, Theorem 1.4.11, p. 19]), an element of $K$ with no zeros also has no poles and must be constant (see [Sti09, Corollary 1.1.20, p. 8]). So for large $n$, we may write $x_n = c_n$ for some $c_n \in F$. Then

$$c_n - 1 = c_n\alpha\beta^{p^{nf}} - \alpha\beta^{p^{(n+1)f}}.$$

As $\beta \notin F$, we may choose a place $Q$ with $v_Q(\beta) > 0$ (again by [Sti09, Corollary 1.1.20, p. 8]). The $Q$-adic valuation of the displayed right side

tends to infinity with $n$, while the $Q$-adic valuation of the left is 0 unless $c_n = 1$. So it must be that $c_n = 1$ for all large $n$. Putting this back into the last equation forces $\beta$ to be a root of unity, contradicting that $\beta \notin F$.

## 3. A sufficient criterion for Schinzel–Wójcik in number fields: Proof of Theorem 1.2

We begin with a simple reduction. Let $\tilde{K}$ be the Galois closure of $K/\mathbb{Q}$. If $P_0$ is a prime of $\mathcal{O}_K$ generous for $K, \alpha, \beta$, and $\tilde{P}_0$ is a prime of $\mathcal{O}_{\tilde{K}}$ lying above $P_0$, then $\tilde{P}_0$ is generous with respect to $\tilde{K}, \alpha, \beta$. Moreover, if $\tilde{P}$ is a nonzero prime ideal of $\mathcal{O}_{\tilde{K}}$ with $v_{\tilde{P}}(\alpha) = v_{\tilde{P}}(\beta) = 0$ and for which $\alpha, \beta$ have the same order in $\mathcal{O}_{\tilde{P}}/\tilde{P}\mathcal{O}_{\tilde{P}}$, then $P = \tilde{P} \cap \mathcal{O}_K$ is a nonzero prime of $\mathcal{O}_K$ where $v_P(\alpha) = v_P(\beta) = 0$ and for which $\alpha, \beta$ have the same order in $\mathcal{O}_P/P\mathcal{O}_P$. The upshot is that, by replacing $K$ with $\tilde{K}$, we can (and will) assume that $K/\mathbb{Q}$ is Galois.

If $\alpha^q = \beta$ for infinitely many primes $q$, then $\alpha$ and $\beta$ are roots of unity in $K$, and they share the same multiplicative order modulo $P$ for *every* nonzero prime ideal $P$. To see this last claim, note that the $q$th power map is an automorphism of $(\mathcal{O}_P/P\mathcal{O}_P)^\times$ as long as $q$ does not divide $N(P) - 1$. So we can assume that $\alpha^q - \beta \in K^\times$ for all sufficiently large primes $q$.

Let $\mathcal{S}$ denote the set of nonzero prime ideals $P$ of $\mathcal{O}_K$ for which $v_P(\alpha) = v_P(\beta) = 0$ and $\alpha, \beta$ share the same order in $(\mathcal{O}_P/P\mathcal{O}_P)^\times$. We assume for a contradiction that $\mathcal{S}$ is finite. Let $\mathcal{T}$ be the (finite) set of prime ideals of $\mathcal{O}_K$ belonging to the support of $\alpha$ or $\beta$.

For each prime $q$, we fix — once and for all — a nonzero prime ideal $Q$ of $\mathcal{O}_K$ lying above $q$. For all large primes $q$, we factor

$$(\alpha^q - \beta)\mathcal{O}_K = \prod_{P \in \mathcal{S}} P^{e_{P,q}} \prod_{P \in \mathcal{T}} P^{e_{P,q}} \prod_{\substack{P:\, v_P(\alpha) = v_P(\beta) = 0 \\ P \notin \mathcal{S}}} P^{e_{P,q}}, \tag{3.1}$$

where each $e_{P,q} = v_P(\alpha^q - \beta)$. We now take norms in (3.1) and analyze the resulting equation modulo $Q$.

To get started, suppose $P$ appears to the nonzero exponent $e_{P,q}$ in the third right-hand product in (3.1). Since $\alpha$ and $\beta$ are $P$-integral, we have $e_{P,q} = v_P(\alpha^q - \beta) \geq \min\{q v_P(\alpha), v_P(\beta)\} \geq 0$. Hence, $e_{P,q} \neq 0$ implies that $e_{P,q} > 0$, leading to the equation $\alpha^q = \beta$ in $\mathcal{O}_P/P\mathcal{O}_P$. Since $P \notin \mathcal{S}$, it must be that $q \mid N(P) - 1$, and therefore $N(P) \equiv 1 \pmod{Q}$. So the third product in (3.1) makes a trivial contribution mod $Q$. If on the other hand $P \in \mathcal{T}$, then straightforward reasoning with the strong triangle inequality

shows that for all large $q$,

$$e_{P,q} = \begin{cases} v_P(\beta) & \text{if } v_P(\alpha) > 0, \\ q v_P(\alpha) & \text{if } v_P(\alpha) < 0, \\ v_P(\beta) & \text{if } v_P(\alpha) = 0 \text{ and } v_P(\beta) < 0, \\ 0 & \text{if } v_P(\alpha) = 0 \text{ and } v_P(\beta) > 0. \end{cases}$$

Therefore, modulo $Q$,

$$\begin{aligned} &N\Big(\prod_{P\in\mathcal{T}} P^{e_{P,q}}\Big) \\ &\quad \equiv \prod_{P:\, v_P(\alpha)>0} N(P)^{v_P(\beta)} \prod_{P:\, v_P(\alpha)<0} N(P)^{q v_P(\alpha)} \prod_{P:\, v_P(\alpha)=0, v_P(\beta)<0} N(P)^{v_P(\beta)} \\ &\quad \equiv \prod_{P:\, v_P(\alpha)>0} N(P)^{v_P(\beta)} \prod_{P:\, v_P(\alpha)<0} N(P)^{v_P(\alpha)} \prod_{P:\, v_P(\alpha)=0, v_P(\beta)<0} N(P)^{v_P(\beta)}. \end{aligned} \tag{3.2}$$

(We are assuming $q$ is large. Hence $q$ is coprime to the norm of any prime in the support of $\alpha$ or $\beta$, and the asserted congruence makes sense in $\mathcal{O}_Q/Q\mathcal{O}_Q$.) The right-hand side of (3.2) is independent of $q$; calling this $\gamma_1$, we have that $\gamma_1 \in \mathbb{Q}^{>0}$ and that $N(\prod_{P\in\mathcal{T}} P^{e_{P,q}}) \equiv \gamma_1 \pmod{Q}$.

We turn now to the left-hand side of (3.1). For each $\tau \in \mathrm{Gal}(K/\mathbb{Q})$, define $\epsilon(\tau) \in K$ by $\epsilon(\tau) = \prod_{\sigma\in\mathrm{Gal}(K/\mathbb{Q})}((\tau\circ\sigma)(\alpha) - \sigma(\beta))$, and let

$$\mathscr{E} = \{\pm\epsilon(\tau) : \tau \in \mathrm{Gal}(K/\mathbb{Q})\}.$$

(The $\pm$ means we include both choices of sign.) If $q$ is sufficiently large, then $v_Q(\sigma(\alpha)) = v_Q(\sigma(\beta)) = 0$ for all $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$, and

$$\begin{aligned} N_{K/\mathbb{Q}}(\alpha^q - \beta) &= \prod_{\sigma\in\mathrm{Gal}(K/\mathbb{Q})} (\sigma(\alpha)^q - \sigma(\beta)) \\ &\equiv \prod_{\sigma\in\mathrm{Gal}(K/\mathbb{Q})} ((\mathrm{Frob}_{Q/q}\circ\sigma)(\alpha) - \sigma(\beta)) \pmod{Q}. \end{aligned}$$

Since $N((\alpha^q - \beta)\mathcal{O}_K) = |N_{K/\mathbb{Q}}(\alpha^q - \beta)|$, we see that $N((\alpha^q - \beta)\mathcal{O}_K) \equiv \epsilon_q \pmod{Q}$ for some $\epsilon_q \in \mathscr{E}$.

It remains to analyze the product over $P \in \mathcal{S}$ appearing in (3.1). Our plan is to restrict $q$ to an arithmetic progression in such a way that the contribution from $P \in \mathcal{S}$ is independent of $q$ and highly divisible by the rational prime $p_0$ lying below $P_0$.

Fix a nonnegative integer $v$ with the property that

$$v > v_{p_0}(\epsilon) - v_{p_0}(\gamma_1) \tag{3.3}$$

for all $\epsilon \in \mathscr{E} \cap \mathbb{Q}^{>0}$. Our hypotheses imply that $\alpha$ and $\beta$ generate the same subgroup of $(\mathcal{O}_{P_0}/P_0^v\mathcal{O}_{P_0})^\times$. Let $\ell$ be the order of that subgroup. If we choose

$n \in \mathbb{Z}$ with $\alpha^n \equiv \beta \pmod{P_0^v}$, then $\gcd(n, \ell) = 1$. Using Dirichlet's theorem on primes in progressions, we fix a prime number $q_0 \equiv n \pmod{\ell}$. We can choose $q_0$ large enough that $\alpha^{q_0} - \beta \neq 0$ and so that $q_0$ is larger than the norm of any prime ideal in $\mathcal{S}$.

Henceforth we restrict attention to primes $q$ satisfying

$$q \equiv q_0 \pmod{\prod_{P \in \mathcal{S}} N(P)^{e_{P,q_0}}(N(P)-1)}. \tag{3.4}$$

(Recall that $e_{P,q_0} = v_P(\alpha^{q_0} - \beta)$; note that $e_{P,q_0}$ is a nonnegative integer for each $P \in \mathcal{S}$, since $\alpha$ and $\beta$ are $P$-integral for all such $P$.) Our choice of $q_0$ is coprime to the modulus, and so the congruence (3.4) holds for infinitely many primes $q$. Furthermore, for any such prime $q$ and any $P \in \mathcal{S}$,

$$N(P)^{e_{P,q_0}}(N(P)-1) \mid q - q_0, \quad \text{so that} \quad \alpha^{q-q_0} \equiv 1 \pmod{P^{1+e_{P,q_0}}},$$

and thus (by the strict triangle inequality)

$$v_P(\alpha^q - \beta) = v_P(\alpha^{q_0}(\alpha^{q-q_0} - 1) + \alpha^{q_0} - \beta) = e_{P,q_0}.$$

Therefore, $N(\prod_{P \in \mathcal{S}} P^{e_{P,q}}) = \gamma_2$ where

$$\gamma_2 := \prod_{P \in \mathcal{S}} N(P)^{e_{P,q_0}} \in \mathbb{Z}^{>0}.$$

Putting everything together, we see that for all large $q$ satisfying the congruence (3.4),

$$\epsilon_q \equiv \gamma_2 \gamma_1 \pmod{Q}.$$

Since the $\epsilon_q$ belong to the fixed finite set $\mathscr{E}$, the same $\epsilon_q$ must appear for infinitely many $q$. This gives $\epsilon = \gamma_2\gamma_1$ for some $\epsilon \in \mathscr{E} \cap \mathbb{Q}^{>0}$. We now obtain a contradiction by considering $p_0$-adic valuations.

Since $P_0 \in \mathcal{S}$, the positive integer $\gamma_2$ satisfies that

$$p_0^{e_{P_0,q_0}} \mid N(P_0)^{e_{P_0,q_0}} \mid \gamma_2.$$

Recall $q_0$ was chosen so that the multiplicative order $\ell$ of $\alpha$ in $(\mathcal{O}_{P_0}/P_0^v\mathcal{O}_{P_0})^\times$ divides $q_0 - n$, where $v_{P_0}(\alpha^n - \beta) \geq v$. It follows that $\alpha^{q_0} \equiv \alpha^n \equiv \beta \pmod{P_0^v}$, and $e_{P_0,q_0} = v_{P_0}(\alpha^{q_0} - \beta) \geq v$. Hence, $v_{p_0}(\gamma_2) \geq v$ and

$$v_{p_0}(\epsilon) = v_{p_0}(\gamma_2) + v_{p_0}(\gamma_1) \geq v + v_{p_0}(\gamma_1).$$

But this contradicts our choice of $v$; see (3.3). This completes the proof of Theorem 1.2.

The following proposition is helpful for producing generous primes.

**Proposition 3.1.** *Let $K$ be a number field and let $\alpha, \beta \in K^\times$. Let $P$ be a degree 1 prime ideal of $\mathcal{O}_K$, unramified over $\mathbb{Q}$, with $v_P(\alpha) = v_P(\beta) = 0$.*

*Let $p = N(P)$. Suppose there exist integers $n$ and $m$ with*

$$v_P(\alpha^n - \beta) \geq v_P(\alpha^{p-1} - 1) \quad \text{and} \quad v_P(\beta^m - \alpha) \geq v_P(\beta^{p-1} - 1). \tag{3.5}$$

*Then $P$ is generous with respect to $K, \alpha, \beta$.*

For use in the proof we quote Lemma 2.1 from [KP23].

**Lemma 3.2.** *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 $k$ with $A^k \equiv B \pmod{p^T}$.*

*Proof of Proposition 3.1.* By the symmetry of the hypotheses, it is enough to show $\alpha$ is a power of $\beta$ modulo $P^v$ for each nonnegative integer $v$. This is clear for all $v \leq v_0 := v_P(\alpha^n - \beta)$. In particular, if $v_0 = \infty$ (i.e., if $\alpha^n = \beta$), there is nothing more to show. Suppose now that $v > v_0$. We will argue that there is an integer $k$ with $\alpha^{n+(p-1)k} \equiv \beta \pmod{P^v}$.

Rearranging, we want $\alpha^{(p-1)k} \equiv \beta\alpha^{-n} \pmod{P^v}$. Identifying the $P$-adic completion of $\mathcal{O}_K$ with $\mathbb{Z}_p$, solvability follows from Lemma 3.2 with $A := \alpha^{p-1}$, $B := \beta\alpha^{-n}$, $t := v_P(\alpha^{p-1} - 1)$ and $T := v$. We use here that $v \geq v_0$ and that $v_0 = v_P(B-1) \geq t$. □

**Example 3.3.** For many choices of $K$, $\alpha$, and $\beta$, the hypotheses of Proposition 3.1 are satisfied with $n = m = 1$ and a degree 1 prime $P$ appearing to a positive power in the factorization of $(\alpha - \beta)\mathcal{O}_K$. Here is a an example where we have to work harder. Let $K = \mathbb{Q}(\sqrt{2}, \sqrt{5})$. Let

$$\alpha = \frac{1+\sqrt{2}}{1-\sqrt{2}}, \quad \beta = \frac{1+\sqrt{5}}{1-\sqrt{5}}.$$

(In this case $(\alpha - \beta)\mathcal{O}_K$ is a prime ideal of degree 2.) Using `gp/PARI` for the computations, one finds that $(\alpha^7 - \beta)\mathcal{O}_K = P_3 P_{53} P_{479} P'_{479}$, where the subscripts on the prime ideal factors indicate the rational primes lying below. Writing $K = \mathbb{Q}(\theta)$ for $\theta = \sqrt{2} + \sqrt{5}$, one can choose the labeling so that $P := P_{479} = (479, \theta - 270)$, which has degree 1 and is unramified over $\mathbb{Q}$. Hensel lifting, one finds that $\theta \equiv 270 + 37 \cdot 479 \pmod{P^2}$. Starting from $\sqrt{2} = \frac{1}{6}(\theta^3 - 11\theta)$ and $\sqrt{5} = -\frac{1}{6}(\theta^3 - 17\theta)$, one finds that $\alpha \equiv 57851 \pmod{P^2}$ and $\beta \equiv 91259 \pmod{P^2}$. This is enough information to verify (3.5) with $n = 7$ and $m = 205$. (Here $m$ was chosen as the inverse of $n$ modulo $N(P) - 1 = 478$.) In fact all the $P$-adic valuations occurring in (3.5) are equal to 1.

**Remark 3.4.** Let $\{u_n\}$ and $\{v_n\}$ be the sequences defined by the initial conditions $u_0 = v_0 = 0$, $u_1 = v_1 = 1$, and the recurrence relations $u_n =$

$2u_{n-1} + u_{n-2}$ and $v_n = v_{n-1} + v_{n-2}$ for integers $n \geq 2$. These are the Pell and Fibonacci numbers, respectively. For a prime $p$, its rank of appearance in either sequence is the smallest positive integer $n$ for which $p$ divides the $n$th term, when such an integer exists. For example, the rank of appearance of 113 in the sequence $\{v_n\}$ is 19, since $113 \mid 4181 = v_{19}$ and 113 does not divide $v_n$ for any positive integer $n < 19$. On the other hand, the rank of appearance of 113 in $\{u_n\}$ is 28.

It is well-known that $u_n$ and $v_n$ admit the Binet formulas $u_n = \frac{1}{2\sqrt{2}}((1+\sqrt{2})^n - (1-\sqrt{2})^n)$ and $v_n = \frac{1}{\sqrt{5}}((\frac{1+\sqrt{5}}{2})^n - (\frac{1-\sqrt{5}}{2})^n)$. (For the general theory of which this is a special case, see [Rib00, Chapter 1].) From these formulas, one sees that if $K$ is any number field containing $\sqrt{2}$ and $\sqrt{5}$, and $P$ is a prime ideal of $K$ lying above a rational prime $p$ not dividing 10, then the rank of appearance of $p$ in $\{u_n\}$ is the order of $\frac{1+\sqrt{2}}{1-\sqrt{2}}$ modulo $P$ while the rank of appearance of $p$ in $\{v_n\}$ is the mod $P$ order of $\frac{1+\sqrt{5}}{1-\sqrt{5}}$. So our last example has the following corollary.

**Corollary 3.5.** *There are infinitely many primes whose rank of appearance in the Pell numbers coincides with its rank of appearance in the Fibonacci numbers.*

**Acknowledgements.** The author is supported by the National Science Foundation (USA) under Award DMS-2001581. He thanks the referee for a thorough reading and useful report. He is also grateful to Pete L. Clark for thoughtful comments on the initial draft.

## References

[JÖ21] O. Järviniemi, *Equality of orders of a set of integers modulo a prime*, Proc. Amer. Math. Soc. 149 (2021), 3651–3668.

[JP23] O. Järviniemi and A. Perucca, *Unified treatment of Artin-type problems*, Res. Number Theory 9 (2023), no. 1, Paper No. 10, 20 pages.

[JP21] M. Just and P. Pollack, *Comparing multiplicative orders mod p, as p varies*, New York J. Math. 27 (2021), 600–614.

[KP23] S. Konyagin and P. Pollack, *A problem in comparative order theory*, Period. Math. Hungar. 86 (2023), 24–36.

[PS95] F. Pappalardi and I. Shparlinski, *On Artin's conjecture over function fields*, Finite Fields Appl. 1 (1995), 399–404.

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

[Rib00] P. Ribenboim, *My numbers, my friends: Popular lectures on number theory*, Springer-Verlag, New York, 2000.

[Ros02] M. Rosen, *Number theory in function fields*, Graduate Texts in Mathematics, vol. 210, Springer-Verlag, New York, 2002.

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

[SW92] A. Schinzel and J. Wójcik, *On a problem in elementary number theory*, Math. Proc. Cambridge Philos. Soc. 112 (1992), 225–232.

[Sti09] H. Stichtenoth, *Algebraic function fields and codes*, second ed., Graduate Texts in Mathematics, vol. 254, Springer-Verlag, Berlin, 2009.

[W96] J. Wójcik, *On a problem in algebraic number theory*, Math. Proc. Cambridge Philos. Soc. 119 (1996), 191–200.

Department of Mathematics, University of Georgia, Athens, Georgia 30601, United States

*Email address*: pollack@uga.edu