ARITHMETIC PROGRESSIONS IN A UNIQUE FACTORIZATION DOMAIN

SUDHIR R. GHORPADE AND SAMRITH RAM

Abstract. Pillai showed that any sequence of consecutive integers with at most 16 terms possesses one term that is relatively prime to all the others. We give a new proof of a slight generalization of this result to arithmetic progressions of integers and further extend it to arithmetic progressions in unique factorization domains of characteristic zero.

1. Introduction

In an attempt to prove a conjecture that products of consecutive integers are never perfect powers, Pillai [16] (see also [19]), in the early 1940's, considered the problem of finding sets of positive integers having the property that they possess an element that is relatively prime to all the rest. He showed that in any set of at most 16 consecutive integers there exists one that is relatively prime to the others. In addition, he proved that for $17 \leq m \leq 430$, there exist infinitely many sets of m consecutive integers which possess no element that is relatively prime to all the rest. Pillai, in fact, believed that the latter result is true for all $m \geq 17$, and this was soon confirmed by Brauer [2] and independently by Pillai himself [17, 18] using a result of Erdős [5, Theorem II]; for more recent proofs, one may refer to Evans [7], Harborth [11], and Eggleton [4]. In what follows, we shall refer to the former result as the Pillai Theorem and the latter as the Brauer-Pillai Theorem.

It is not difficult to show that the Pillai Theorem is applicable not only to sets of at most 16 consecutive integers, but also to arithmetic progressions of integers with at most 16 terms, and we will refer to this fact as the Generalized Pillai Theorem. While we have not found in the existing literature a proof of this fact (see, however, Remark 3.3), analogues of the Brauer-Pillai Theorem for arithmetic progressions are readily found, and we cite, in particular, the works of Evans [8], Ohtomo and Tamari [14], and

Date: March 12, 2012.

2010 *Mathematics Subject Classification.* Primary 11B25, 13F15; Secondary 11A05, 13A05.

Key words and phrases. Consecutive integers, arithmetic progressions, unique factorization domain, Bézout domain, GCD domain, decomposition number.

of Hajdu and Saradha [10]. Moreover, numerous extensions, analogues and generalizations of the Brauer-Pillai Theorem have been considered in the recent past; see, for example, Caro [3], Gassko [9], Saradha and Thangadurai [20], and also the works cited above. It may be remarked that all these extensions are in the setting of integers and use techniques from elementary or analytic number theory.

We consider in this paper an extension of the Generalized Pillai Theorem in a wider algebraic context. Thus, we ask, if a similar result holds for Gaussian integers, or more generally, for rings of integers of algebraic number fields of class number one, or even more generally, for arbitrary integral domains where the notion of GCD (and hence of two elements being relatively prime) makes sense. Our main result is an analogue of the Generalized Pillai Theorem for the so-called σ-atomic GCD domains of characteristic zero, and in particular, for arbitrary unique factorization domains of characteristic zero. This is achieved partly by introducing an invariant associated to an integral domain, called its *decomposition number*. It is then proved that if R is a UFD of characteristic zero with decomposition number δ_R and if $N := \min\{16, 1 + \delta_R\}$, then any arithmetic progression of at most N terms with the first term coprime to the common difference contains a term that is relatively prime to all the rest. It is also shown that $N := \min\{16, 1 + \delta_R\}$ is the maximum possible number with this property. As a special case, one sees that the Generalized Pillai Theorem holds for the Gaussian integers with 16 replaced by 6. Our proof of the general result makes use of the corresponding result for integers. With this in view, and in a bid to make this paper self-contained, we include in Section 2 below a fairly short proof of the Generalized Pillai Theorem for arithmetic progressions of integers, which gives, in particular, a new proof of the Pillai Theorem. Some ring theoretic preliminaries and the notion of decomposition number are discussed in Section 3. The main result is proved in Section 4.

2. Arithmetic Progressions of Integers

Let us begin with some notations and terminology, which will be used in the remainder of this paper. Let R be an integral domain. For $r \in R$ and $S \subseteq R$, we denote by $\mathsf{M}(r, S)$ the set $\{s \in S : r \mid s\}$ of all multiples of r in S. For $a, d \in R$ and a positive integer n, we denote by $\mathsf{AP}(a, d, n)$ the set $\{a, a+d, \ldots, a+(n-1)d\}$ of elements of the arithmetic progression with n terms having a as its first term and d the common difference. Further, if R is a GCD domain (i.e. an integral domain in which any two elements have a greatest common divisor) and m, n are positive integers, then we shall write $\{a_1, a_2, \ldots, a_m\} \perp \{b_1, b_2, \ldots, b_n\}$ to mean that $\gcd(a_i, b_j) = 1$ for $1 \le i \le m$ and $1 \le j \le n$. Here, as usual, $\gcd(a, b)$ denotes a greatest common divisor of $a, b \in R$, and although it is determined only up to multiplication by a unit, statements such as "$\gcd(a, b) = 1$" or "$\gcd(a, b)$ divides c" have an unambiguous and obvious meaning, and we shall continue to use them. Of course if $R = \mathbb{Z}$ is the ring of integers, then $\gcd(a, b)$ is unique since we require it to be positive if $a, b \in \mathbb{Z}$ are not both zero and set $\gcd(0, 0) := 0$. Also if $R = \mathbb{Z}$ and n is a positive integer, then $\le$ will denote the componentwise partial order on $\mathbb{Z}^n$ so that for any $a_1, \ldots, a_n, b_1, \ldots, b_n \in \mathbb{Z}$, $(a_1, \ldots, a_n) \le (b_1, \ldots, b_n) \iff a_i \le b_i$ for all $i = 1, \ldots, n$. Finally, for a finite set A, we denote by $|A|$ the cardinality of A.

Theorem 2.1 (Generalized Pillai Theorem)**.** Let a, d be coprime integers and let n be a positive integer ≤ 16. Then the arithmetic progression $a, a + d, \ldots, a + (n-1)d$ contains a term that is relatively prime to all the others.

We first make an elementary observation and record a useful consequence thereof.

Lemma 2.2. If R is a GCD domain, $a, d \in R$ are coprime and r, s are nonnegative integers, then

$$\gcd(a + rd, a + sd) \mid (r - s).$$

Proof. Any common divisor of $a+rd$ and $a+sd$ divides both $(a+rd)-(a+sd)$ and $s(a + rd) - r(a + sd)$. Since $\gcd(a, d) = 1$, the lemma follows. $\square$

Corollary 2.3. If a, d are coprime integers and m is a positive integer, then

$$|\mathsf{M}(m, \mathsf{AP}(a, d, n))| \le \lceil n/m \rceil$$

where $\lceil x \rceil$ denotes the least integer $\ge x$.

We now proceed to prove Theorem 2.1. For $n = 1$, the theorem is vacuously true. Let us first consider the case in which all terms of $\mathsf{AP}(a, d, n)$ are odd. The case where $n = 2$ is trivial. If $n = 3, 4$ or 5, then the term $a + 2d$ is relatively prime to all the others. If $n = 6$, then one of $a + 2d, a + 3d$ is not divisible by 3 and is relatively prime to all the other terms. If $n = 7, 8, 9, 10$ or 11, one of $a + 4d$, $a + 5d$, $a + 6d$ is coprime to both 3 and 5 and consequently is relatively prime to all the other terms. If $12 \le n \le 16$, some element in the set $\{a + id : 6 \le i \le 10\}$ is coprime to 3, 5 and 7 and is relatively prime to all the others in $\mathsf{AP}(a, d, n)$. Thus Theorem 2.1 holds whenever all terms of $\mathsf{AP}(a, d, n)$ are odd, or equivalently, when d is even.

It remains to consider the case when terms in the progression are alternately even and odd. The case where $n = 2$ is trivial. If $n = 3$, the term $a + d$ is relatively prime to the others. If $n = 4$ or 5, at least two terms in the progression are odd and one of those is not divisible by 3. This number is relatively prime to the others. To settle the remaining cases, the following two lemmas will be useful.

Lemma 2.4. Let k be an integer with $3 \le k \le 8$. Suppose Theorem 2.1 holds for any coprime integers a, d with d odd and for $n = 2k - 1$. Then it also holds for any coprime integers a, d with d odd and for $n = 2k$.

Proof. Let a, d be coprime integers with d odd. Write $a_i := a + (i-1)d$ for $i = 1, \dots, 2k$ and $A := \mathsf{AP}(a, d, 2k) = \{a_1, \dots, a_{2k}\}$. Assume first that a_1 is odd. Now $A \setminus \{a_1\} = \mathsf{AP}(a_2, d, 2k-1)$ and hence there exists $m \in \mathbb{Z}$ with $2 \le m \le 2k$ such that $a_m \perp A \setminus \{a_1, a_m\}$. This implies that $a_m \perp \{1, \dots, m-2\}$. Moreover, m is odd since both a_1, d are odd and $k \ge 3$. Consequently, $\gcd(a_1, a_m) \mid (m-1)/2$. On the other hand, $1 \le (m-1)/2 \le m-2$, since $m \ge 3$. It follows that $\gcd(a_m, (m-1)/2) = 1$ and therefore $\gcd(a_1, a_m) = 1$. As a result, $a_m \perp A \setminus \{a_m\}$. In case a_1 is even, a_{2k} is odd and we use the same argument for $\mathsf{AP}(a_{2k}, -d, 2k)$. □

Lemma 2.5. Let k be an integer with $3 \le k \le 7$. Suppose Theorem 2.1 holds for any odd coprime integers a, d and for $n = 2k$. Then it holds for any odd coprime integers a, d and for $n = 2k + 1$.

Proof. The proof is similar to that of Lemma 2.4. Let a, d be odd coprime integers. Write $a_i = a + (i-1)d$ for $i = 1, \dots, 2k+1$ and $A = \mathsf{AP}(a, d, 2k+1)$. By the hypothesis, there exists $m \in \mathbb{Z}$ with $2 \le m \le 2k+1$ such that $a_m \perp A \setminus \{a_1, a_m\}$. This implies that $a_m \perp \{1, \dots, m-2\}$. Moreover, m is odd, $\gcd(a_1, a_m) \mid (m-1)/2$, and $(m-1)/2 \le m-2$, since $m \ge 3$. Thus $\gcd(a_m, a_1) = 1$ and $a_m \perp A \setminus \{a_m\}$. □

In view of the two lemmas above and the discussion preceding it, it suffices to prove the theorem for coprime integers a, d with a even, d odd, and for odd integers n with $7 \le n < 16$. Fix such a, d, n and let $a_i := a + (i-1)d$ for $i = 1, \dots, n$ and $A := \mathsf{AP}(a, d, n) = \{a_1, \dots, a_n\}$. We now proceed by a case-by-case argument.

First, suppose $n = 7$. Let $B := \{a_2, a_4, a_6\} = \mathsf{AP}(a_2, 2d, 3)$. By Corollary 2.3, $|\mathsf{M}(3, B) \cup \mathsf{M}(5, B)| \le 2 < |B|$. Hence it follows that there exists $x \in B$ such that $x \perp \{2, 3, 5\}$. Consequently, $x \perp A \setminus \{x\}$.

Next, suppose $n = 9$. Let $B := A \setminus \mathsf{M}(2, A) = \mathsf{AP}(a_2, 2d, 4)$. By Corollary 2.3,

$$(|\mathsf{M}(3, B)|, |\mathsf{M}(5, B)|, |\mathsf{M}(7, B)|) \leq (2, 1, 1).$$

Since $|B| = 4$, if there is a strict inequality in one of the coordinates, then there is $x \in B$ such that $x \perp \{2, 3, 5, 7\}$ and consequently $x \perp A \setminus \{x\}$. If equality holds in all the coordinates, then $|\mathsf{M}(3, B)| = 2$ and we must necessarily have $\mathsf{M}(3, B) = \{a_2, a_8\}$. But then $\{a_4, a_6\} \perp \{2, 3\}$ and the one among a_4 and a_6 that is coprime to 5 is relatively prime to all other elements in A.

For $n = 11$, let $B := A \setminus \mathsf{M}(2, A) = \mathsf{AP}(a_2, 2d, 5)$. By Corollary 2.3,

$$(|\mathsf{M}(3, B)|, |\mathsf{M}(5, B)|, |\mathsf{M}(7, B)|) \leq (2, 1, 1).$$

Since $2 + 1 + 1 < 5 = |B|$, there exists $x \in B$ with $x \perp \{2, 3, 5, 7\}$ and so $x \perp A \setminus \{x\}$.

We now consider the case $n = 13$. Let $B := A \setminus \mathsf{M}(2, A) = \mathsf{AP}(a_2, 2d, 6)$. Then $|B| = 6$ and by Corollary 2.3,

$$(|\mathsf{M}(3, B)|, |\mathsf{M}(5, B)|, |\mathsf{M}(7, B)|, |\mathsf{M}(11, B)|) \leq (2, 2, 1, 1).$$

If there is a strict inequality in one of the coordinates we are through. So suppose equality holds in all coordinates. This forces $\mathsf{M}(5, B) = \{a_2, a_{12}\}$. So if we let $B_1 := \{a_4, a_6, a_8\}$, then $B_1 \perp \{2, 5\}$ and by Corollary 2.3, $(|\mathsf{M}(3, B_1)|, |\mathsf{M}(7, B_1)|) \leq (1, 1)$. Thus there exists $x \in B_1$ such that $x \perp \{2, 3, 5, 7\}$ and hence $x \perp A \setminus \{x\}$.

Finally, suppose $n = 15$. Let $B := A \setminus (\mathsf{M}(2, A) \cup \{a_2, a_{14}\}) = \mathsf{AP}(a_4, 2d, 5)$. Then $|B| = 5$ and by Corollary 2.3,

$$(|\mathsf{M}(3, B)|, |\mathsf{M}(5, B)|, |\mathsf{M}(7, B)|, |\mathsf{M}(11, B)|) \leq (2, 1, 1, 1).$$

If there is a strict inequality in one of the coordinates or if

$$|\mathsf{M}(3, B) \cup \mathsf{M}(5, B) \cup \mathsf{M}(7, B) \cup \mathsf{M}(11, B)| < 5,$$

then we are through. So suppose equality holds in all coordinates and the four sets $\mathsf{M}(j, B)$, $j = 3, 5, 7, 11$, are disjoint. Let $B_1 := \{a_2, a_{14}\}$. Note that $\mathsf{M}(3, B_1) = \emptyset$. If $\mathsf{M}(5, B_1) = \emptyset$, then $B_1 \perp \{2, 3, 5, 7, 11\}$ and since $|\mathsf{M}(13, B_1)| \leq 1$, some element of B_1 is coprime to all the other elements in A. If $|\mathsf{M}(5, B_1)| = 1$, then $|\mathsf{M}(3, \{a_4, a_{12}\})| = |\mathsf{M}(5, \{a_4, a_{12}\})| = 1$. Consequently, there is $x \in \{a_6, a_8, a_{10}\}$ such that $11 \mid x$, and hence $x \perp \{2, 3, 5, 7\}$. It follows that $x \perp A \setminus \{x\}$. This completes the proof of Theorem 2.1.

Corollary 2.6 (Pillai)**.** In any sequence of at most 16 consecutive integers, there exists an element that is relatively prime to all the others.

Proof. This is just the case $d = 1$ of Theorem 2.1. □

Recall that an integer is said to be a *perfect power* if it is of the form t^r where t and r are integers > 1.

Corollary 2.7. Suppose a, d are coprime positive integers and n is a positive integer ≤ 16 such that no term of $\mathsf{AP}(a, d, n)$ is a perfect power. Then the product $\prod_{k=0}^{n-1}(a + kd)$ is not a perfect power.

Proof. The case $n = 1$ is trivial. If $n \geq 2$, then by Theorem 2.1, there is a term x in $\mathsf{AP}(a, d, n)$ that is coprime to the other terms. If $x > 1$, then the desired result is clear since x is not a perfect power. In case $x = 1$, we must have $a = 1$ and so one can apply Theorem 2.1 to $\mathsf{AP}(a + d, d, n - 1)$. □

Remark 2.8. The hypothesis above that no term of $\mathsf{AP}(a, d, n)$ is a perfect power is crucial since one can find infinitely many arithmetic progressions (with the first term coprime to the common difference) with 3 terms each of which is a square. This follows from the fact that there are infinitely many rational points on the curve $x^2 + y^2 = 2$. For instance, $\{1, 5^2, 7^2\}, \{7^2, 13^2, 17^2\}$ and $\{17^2, 53^2, 73^2\}$.

Remark 2.9. A remarkable theorem of Erdős and Selfridge [6] says that the product of two or more consecutive positive integers is never a perfect power.

Remark 2.10. As mentioned in the Introduction, for each $n > 16$ there exist blocks of n consecutive integers such that they contain no integer relatively prime to all the rest. We refer to Evans [7] for an elegant proof of this result.

3. GCD domains and Decomposition Numbers

The notion of a GCD domain was recalled in the Introduction. Let us also recall that an integral domain R is said to be a *Bézout domain* if every finitely generated ideal of R is principal, while it is said to be *atomic* if every nonzero nonunit in R factors into a product of irreducible elements. In analogy with the latter, we shall say that an integral domain R is *σ-atomic* if every nonzero nonunit in R is divisible by an irreducible element. Evidently, a unique factorization domain (UFD) is a σ-atomic (in fact, atomic) GCD domain. The following example shows that the converse is not true.

Example 3.1. Let R be the ring of entire functions, i.e., complex-valued holomorphic functions on $\mathbb{C}$. The units of R are precisely the entire functions with no zeros in $\mathbb{C}$ and the irreducible elements are given, up to multiplication by units, by the linear polynomials. Thus it is readily seen that R is a σ-atomic domain. Moreover, R is also a GCD domain, and in fact, a Bézout domain, thanks to a result of Helmer [12] (which was, incidentally, published in the same year as Pillai [16]). On the other hand, since there do exist entire functions with infinitely many zeros (e.g., $\sin z$), we see that R is not a UFD. More generally, if R' is any subring of R such that R' strictly contains the subring of R consisting of the polynomial functions, then R' is a σ-atomic GCD domain that is not a UFD. To generate more examples, it suffices to observe that if S is a σ-atomic GCD domain that is not a UFD, then the polynomial ring $S[X]$ is also a σ-atomic GCD domain that is not a UFD; moreover, it is not difficult to see that $S[X]$ is neither Noetherian nor Bèzout.

In the sequel, the following version of Chinese Remainder Theorem will turn out to be useful. A proof when $R = \mathbb{Z}$ can be found in the book of Ore [15, §10–3] and it extends easily to the case when R is any Bézout domain, or more generally, a GCD domain where the moduli satisfy a Bézout hypothesis such as (3.1) below.

Lemma 3.2 (Generalized Chinese Remainder Theorem)**.** Let R be a GCD domain, m be a positive integer, and let $u_i, v_i \in R$ with $v_i \neq 0$ for $i = 1, \dots, m$. Assume that

$$\gcd(v_i, v_j) \in Rv_i + Rv_j \quad \text{for } 1 \le i, j \le m. \tag{3.1}$$

Then the system $z \equiv u_i \pmod{v_i}$, $i = 1, \dots, m$, of m congruences possesses a solution in R if and only if $\gcd(v_i, v_j) \mid (u_i - u_j)$ for $1 \le i, j \le m$.

Remark 3.3. As an application of Lemma 3.2, let us show that the Pillai Theorem (Corollary 2.6) and the Generalized Pillai Theorem (Theorem 2.1) can be deduced from each other. To prove the nontrivial implication, let a, d be coprime integers and n be a positive integer ≤ 16. Write $a_i = a + (i-1)d$ for $i = 1, \dots, n$. By Lemma 2.2, $\gcd(a_i, a_j) \mid i - j$ for $1 \le i, j \le n$. Hence by Lemma 3.2, there is $z \in \mathbb{Z}$ such that $a_i \mid z - i$ for $i = 1, \dots, n$. Now by Corollary 2.6, there is $k \in \{1, \dots, n\}$ such that $z - k$ is relatively prime to $z - j$ for all $j = 1, \dots, n$ with $j \neq k$. Consequently, a_k is relatively prime to a_j for all $j \neq k$.

It is not difficult to show that in a GCD domain, irreducible elements are always prime. In what follows, prime elements of an arbitrary integral domain may simply be referred to as primes, and this terminology should not be confused with prime ideals. Also, following the standard conventions of number theory, we will use the term rational prime to mean a (positive) prime number in $\mathbb{Z}$. Now here is a definition that will play a crucial role in the proof of our main theorem.

Definition 3.4. Let $\mathfrak{R}$ be an integral domain with multiplicative identity $1_{\mathfrak{R}}$. The *decomposition number* of $\mathfrak{R}$, denoted by $\delta_{\mathfrak{R}}$, is the smallest rational prime p such that $p \cdot 1_{\mathfrak{R}}$ is divisible by at least two distinct (i.e., up to multiplication by units) prime elements in $\mathfrak{R}$. If no prime in $\mathbb{Z}$ is divisible by two distinct primes in $\mathfrak{R}$, then we define $\delta_{\mathfrak{R}}$ to be ∞.

It seems worthwhile to illustrate this notion with several examples.

Examples 3.5. (i) Clearly, $\delta_{\mathbb{Z}} = \infty$. Also, if K is a field, then $\delta_K = \infty$.

(ii) If A is an integral domain, then $\delta_{A[[X]]} = \delta_{A[X]} = \delta_A$.

(iii) If R is the ring of entire functions, then $\delta_R = \infty$.

(iv) Suppose $\mathfrak{R} = \mathbb{Z}[\alpha]$ is a UFD for some complex number α satisfying a monic irreducible polynomial $f(X) \in \mathbb{Z}[X]$. Then using a well-known result of Kummer-Dedekind, we see that $\delta_{\mathfrak{R}}$ is the smallest rational prime p such that the image of $f(X)$ in $\mathbb{Z}/p\mathbb{Z}[X]$ is divisible by two distinct irreducible polynomials in $\mathbb{Z}/p\mathbb{Z}[X]$. The next two examples are special cases of this.

(v) Let $K = \mathbb{Q}(\sqrt{m})$ for some squarefree $m \in \mathbb{Z}$ such that $\mathfrak{R} = \mathcal{O}_K$ is a UFD. If $m \equiv 1 (\mathrm{mod}\ 8)$, then $\delta_{\mathfrak{R}} = 2$ and for other values of m, $\delta_{\mathfrak{R}}$ is the smallest rational prime p such that p is odd and $\left(\frac{m}{p}\right) = 1$. (Here $\left(\frac{\cdot}{\cdot}\right)$ denotes the *Legendre symbol*). In particular, $\delta_{\mathbb{Z}[i]} = 5$.

(vi) Suppose ζ_m is a primitive m-th root of unity such that $\mathfrak{R} = \mathbb{Z}[\zeta_m]$ is a UFD. (The precise values of m for which $\mathbb{Z}[\zeta_m]$ is a UFD are known; cf. [13]). For any rational prime p, let $p^{v_p(m)}$ be the highest power of p dividing m and let $\ell(m,p) := m/p^{v_p(m)}$. Then from [1, Theorem 2], we see that $\delta_{\mathfrak{R}}$ is the smallest rational prime p for which $\ell(m,p) > 1$ and p is not a primitive root modulo $\ell(m,p)$.

4. Arithmetic Progressions in GCD domains

For an integral domain $\mathfrak{R}$, we shall denote by $\mathbb{Z}_{\mathfrak{R}}$ the prime subring of $\mathfrak{R}$. In case $\mathfrak{R}$ is of characteristic zero, $\mathbb{Z}_{\mathfrak{R}}$ can be identified with $\mathbb{Z}$.

Theorem 4.1. Let $\mathfrak{R}$ be a σ-atomic GCD domain of characteristic 0. Then we have the following:

(i) If n is a positive integer $\leq \min\{16, 1+\delta_{\mathfrak{R}}\}$, then for any coprime $a, d \in \mathfrak{R}$, the arithmetic progression $\mathsf{AP}(a,d,n)$ contains a term that is relatively prime to all the others.

(ii) Assume that no prime of $\mathbb{Z}_{\mathfrak{R}}$ is a unit in $\mathfrak{R}$. Then for each integer n with $n > \min\{16, 1+\delta_{\mathfrak{R}}\}$, there exists an arithmetic progression $\mathsf{AP}(a,d,n)$ in $\mathfrak{R}$, where $a, d \in \mathfrak{R}$ are coprime, such that none of its terms is relatively prime to all the others.

Proof. (i) Assume, on the contrary, that $n \leq \min\{16, 1+\delta_{\mathfrak{R}}\}$ and that there exists an arithmetic progression $a_1, \ldots, a_n$ in $\mathfrak{R}$ with $\gcd(a_1, a_2) = 1$ such that no term is relatively prime to the rest. Let $d = a_2 - a_1$. For each i there exists a j_i such that a_i is not coprime to a_{j_i}. Then there exists a prime P_i dividing $\gcd(a_i, a_{j_i})$. Let π be the product of the distinct primes in $\{P_1, \ldots, P_n\}$, say

$$\pi = P_{i_1} P_{i_2} \cdots P_{i_k}.$$

Let $r_i = \gcd(\pi, a_i)$. Note that no r_i is relatively prime to all the $r_j (j \neq i)$. For any prime $P \in \mathfrak{R}$ let $I_P = \{i : P \mid r_i\}$. Suppose

$$\bigcup_{j=1}^{k} \{I_{P_{i_j}}\} = \{I_{Q_1}, I_{Q_2}, \cdots, I_{Q_l}\}.$$

where each Q_m is one of the P_{i_j}. Now define

$$s_i = \gcd(r_i, Q_1 \cdots Q_l) \quad (1 \leq i \leq n).$$

Again note that no s_i is relatively prime to all the $s_j (j \neq i)$. By the choice of the s_i, it follows that if $Q_s \neq Q_t$, then

$$|\{i : Q_s \mid s_i\}| \geq 2 \quad \text{ and } \quad \{i : Q_s \mid s_i\} \neq \{i : Q_t \mid s_i\}.$$

Note that $a_i \equiv 0 \pmod{s_i}$. If P is a prime dividing some s_l, then P also divides some $s_m (l \neq m)$. Then $P \mid (l-m)1_{\mathfrak{R}}$. If $p \in \mathbb{Z}$ is the positive prime such that $P\mathfrak{R} \cap \mathbb{Z}_{\mathfrak{R}} = p\mathbb{Z}_{\mathfrak{R}}$, then it follows that $p \mid (l-m)$. Thus $p \leq n-1 \leq \delta_{\mathfrak{R}}$. This implies that each $s_i (1 \leq i \leq n)$ is a product of primes each of which lies over $p \cdot 1_{\mathfrak{R}}$ for some positive prime $p \in \mathbb{Z}$ not exceeding $\delta_{\mathfrak{R}}$. Also, any prime P lying over $\delta_{\mathfrak{R}} \cdot 1_{\mathfrak{R}}$ can appear in the factorization of some s_m only if $n = \delta_{\mathfrak{R}} + 1$ and in this case P necessarily divides both s_1 and s_n and no other s_i. Also, in this case no other prime $Q \in \mathfrak{R}$ lying over $\delta_{\mathfrak{R}} \cdot 1_{\mathfrak{R}}$ can divide s_1 or s_n (since $\{i : P \mid s_i\} \neq \{i : Q \mid s_i\}$). Now, the system

$$z \equiv -(i-1)d \pmod{s_i} \quad 1 \leq i \leq n$$

possesses a solution, namely $z = a_1$ in $\mathfrak{R}$. This implies that

$$\gcd(s_i, s_j) \mid (i-j)d \cdot 1_{\mathfrak{R}} \quad 1 \leq i, j \leq n.$$

Also note that $\gcd(s_i, d) = 1$ for all i (otherwise the fact that the first term is coprime to the common difference is contradicted). Thus we have

$$\gcd(s_i, s_j) \mid (i-j) \cdot 1_{\mathfrak{R}} \quad 1 \le i, j \le n. \tag{4.1}$$

For each i let $t_i \in \mathbb{Z}$ denote the unique positive integer such that $s_i\mathfrak{R} \cap \mathbb{Z}_{\mathfrak{R}} = t_i\mathbb{Z}_{\mathfrak{R}}$. Let $t_{ij} = \gcd(t_i, t_j)$ and $s_{ij} = \gcd(s_i, s_j)$. Then $t_{ij} \in t_i\mathbb{Z}_{\mathfrak{R}} + t_j\mathbb{Z}_{\mathfrak{R}}$ and consequently

$$s_{ij} \in \mathfrak{R}s_i + \mathfrak{R}s_j. \tag{4.2}$$

From (4.1) and (4.2) together with Lemma 3.2, it follows that the system

$$z \equiv (1-i)1_{\mathfrak{R}} \pmod{s_i}, \quad i = 1, \ldots, n,$$

possesses a solution in $\mathfrak{R}$. By the choice of s_i and t_i it is easily seen that

$$s_{ij}\mathfrak{R} \cap \mathbb{Z}_{\mathfrak{R}} = t_{ij}\mathbb{Z}_{\mathfrak{R}}.$$

Consequently

$$\gcd(t_i, t_j) \mid (i-j) \text{ for } 1 \le i, j \le n$$

and so by Lemma 3.2, the system

$$z \equiv 1 - i \pmod{t_i}, \quad i = 1, \ldots, n,$$

possesses a solution, say x, in $\mathbb{Z}$. Note that no t_i is relatively prime to all the others. Now $x, x+1, \ldots, x+n-1$ is a sequence of n consecutive integers such that none of them is relatively prime to all the rest. Hence by Corollary 2.6, $n > 16$, which is a contradiction. This proves (i).

(ii) If $n > 16$, then by Remark 2.10 there exists an arithmetic progression $\mathsf{AP}(a, d, n)$ in $\mathbb{Z}$ (and hence in $\mathbb{Z}_{\mathfrak{R}}$) such that none of its terms is relatively prime to all the others. Since no prime in $\mathbb{Z}_{\mathfrak{R}}$ is a unit in $\mathfrak{R}$ we are through. So we only need to consider progressions where $1+\delta_{\mathfrak{R}} < n < 17$. For $\delta_{\mathfrak{R}} < 17$ let P, Q be distinct primes in $\mathfrak{R}$ dividing $\delta_{\mathfrak{R}}1_{\mathfrak{R}}$. Let $z \in \mathfrak{R}$ be a solution of the system

$$\begin{aligned} z &\equiv 0 \left(\bmod\ 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot \frac{P}{\delta_{\mathfrak{R}}}\right) \\ z + 1_{\mathfrak{R}} &\equiv 0 \pmod{Q}. \end{aligned}$$

Then for $1 + \delta_{\mathfrak{R}} < n < 17$, we claim that the progression $z,\ z+1_{\mathfrak{R}},\ \ldots,\ z+(n-1)1_{\mathfrak{R}}$ contains no term relatively prime to all the others. Indeed, z and $z+1_{\mathfrak{R}}$ share a common factor with $z+\delta_{\mathfrak{R}}1_{\mathfrak{R}}$ and $z+(\delta_{\mathfrak{R}}+1)1_{\mathfrak{R}}$ respectively, whereas all other terms in the progression share a common factor with either z or $z+1_{\mathfrak{R}}$. This completes the proof of Theorem 4.1. $\square$

Remark 4.2. In part (i) of Theorem 4.1, the hypothesis that $\mathfrak{R}$ is σ-atomic is crucial. For example, if $\mathfrak{R}$ is the ring $\mathbb{A}$ of all algebraic integers (all complex numbers integral over $\mathbb{Z}$), then $\delta_{\mathbb{A}} = \infty$ since there are no prime elements in $\mathbb{A}$. However, the progression

$$\frac{\sqrt{17}+3}{2}, \frac{\sqrt{17}+5}{2}, \frac{\sqrt{17}+7}{2}, \frac{\sqrt{17}+9}{2}$$

contains no element coprime to the others. Also, in part (ii) of Theorem 4.1, the assumption that no prime in $\mathbb{Z}$ is a unit in $\mathfrak{R}$ is necessary. For example, if $\mathfrak{R}$ is a field, then every arithmetic progression in $\mathfrak{R}$ with at least one nonzero term contains a term that is relatively prime to all the others.

Remark 4.3. Note that only values of $\delta_{\mathfrak{R}} \leq 13$ can affect the permissible values of n such that $\mathsf{AP}(a, d, n)$ contains a term coprime to the others. For the purposes of the above theorem it is unnecessary to determine $\delta_{\mathfrak{R}}$ if it is known to be greater than 13 (this of course includes the case $\delta_{\mathfrak{R}} = \infty$).

Definition 4.4. An element of an integral domain R is said to be a *perfect power* if it can be expressed in the form t^r where t is a nonzero, non-unit in R and r is a positive integer > 1.

Corollary 4.5. Let $\mathfrak{R}$ be a UFD of characteristic 0 and $a, d \in \mathfrak{R}$ be coprime. If n is a positive integer $\leq \min\{16, 1 + \delta_{\mathfrak{R}}\}$ and if $\mathsf{AP}(a, d, n)$ contains no units and no perfect powers, then the product $\prod_{k=0}^{n-1}(a + kd)$ is not a perfect power.

Proof. If some term of $\mathsf{AP}(a, d, n)$ is zero, then so is the product and 0 is not a perfect power, by definition. Otherwise, the result follows readily from Theorem 4.1. ∎

References

[1] G. Bachman, *The decomposition of a rational prime ideal in cyclotomic fields*, Amer. Math. Monthly **73** (1966), 494–497.

[2] A. Brauer, *On a property of k consecutive integers*, Bull. Amer. Math. Soc. **47** (1941), 328–331.

[3] Y. Caro, *On a division property of consecutive integers*, Israel J. Math. **33** (1979), no. 1, 32–36.

[4] R. B. Eggleton, *Common factors of integers: a graphic view*, Discrete Math. **65** (1987), no. 2, 141–147.

[5] P. Erdős, *On the difference of consecutive primes*, Quart. J. Math. **6** (1935), 124–128.

[6] P. Erdős and J. L. Selfridge, *The product of consecutive integers is never a power*, Illinois J. Math. **19** (1975), 292–301.

[7] R. J. Evans, *Mathematical Notes: On Blocks of N Consecutive Integers*, Amer. Math. Monthly **76** (1969), no. 1, 48–49.

[8] R. J. Evans, *On N consecutive integers in an arithmetic progression*, Acta Sci. Math. (Szeged) **33** (1972), 295–296.

[9] I. Gassko, *Stapled sequences and stapling coverings of natural numbers*, Electron. J. Combin. **3** (1996), no. 1, Research Paper 33, approx. 20 pp. (electronic).

[10] L. Hajdu and N. Saradha, *On a problem of Pillai and its generalizations*, Acta Arith. **144** (2010), 323-347.

[11] H. Harborth, *Eine Eigenschaft aufeinanderfolgender Zahlen*, Arch. Math. (Basel) **21** (1970), 50–51.

[12] O. Helmer, *Divisibility properties of integral functions*, Duke Math. J. **6** (1940), 345–356.

[13] J. Myron Masley and H. L. Montgomery, *Cyclotomic fields with unique factorization*, J. Reine Angew. Math. **286/287** (1976), 248–256.

[14] M. Ohtomo and F. Tamari, *On relative prime number in a sequence of positive integers*, J. Statist. Plann. Inference **106** (2002), no. 1-2, 509–515.

[15] Oystein Ore, *Number Theory and Its History*, McGraw-Hill Book Company, Inc., New York, 1948.

[16] S. S. Pillai, *On m consecutive integers I*, Proc. Indian Acad. Sci., Sect. A. **11** (1940), 6–12.

[17] S. S. Pillai, *On m consecutive integers III*, Proc. Indian Acad. Sci., Sect. A. **13** (1941), 530–533.

[18] S. S. Pillai, *On m consecutive integers IV*, Bull. Calcutta Math. Soc. **36** (1944), 99–101.

[19] S. S. Pillai, *Collected works of S. Sivasankaranarayana Plliai*, Eds. R. Balasubramanian and R. Thangadurai, Collected Works Series, no. 1, Ramanujan Mathematical Society, Mysore, 2010.

[20] N. Saradha and R. Thangadurai, *Pillai's problem on consecutive integers*, Number theory and applications, Hindustan Book Agency, New Delhi, 2009, pp. 175–188.

Department of Mathematics, Indian Institute of Technology Bombay, Powai, Mumbai 400076, India.
E-mail address: srg@math.iitb.ac.in

Department of Mathematics, Indian Institute of Technology Bombay, Powai, Mumbai 400076, India.
E-mail address: samrith@gmail.com