J. Austral. Math. Soc. (*Series A*) **63** (1997), 396–420

ON A CONJECTURE OF CRITTENDEN AND VANDEN EYNDEN CONCERNING COVERINGS BY ARITHMETIC PROGRESSIONS

R. J. SIMPSON

(Received 12 August 1996)

Communicated by W. W. L. Chen

Abstract

Crittenden and Vanden Eynden conjectured that if n arithmetic progressions, each having modulus at least k, include all the integers from 1 to $k2^{n-k+1}$, then they include all the integers. They proved this for the cases $k = 1$ and $k = 2$. We give various necessary conditions for a counterexample to the conjecture; in particular we show that if a counterexample exists for some value of k, then one exists for that k and a value of n less than an explicit function of k.

1991 *Mathematics subject classification* (*Amer. Math. Soc.*): 11B25.
Keywords and phrases: arithmetic progressions, covering systems.

1. Introduction

We will use the following notation. $S(m, a)$ is the set of integers x satisfying $x \equiv a \pmod{m}$. We will refer to $S(m, a)$ as an *arithmetic progression*, although strictly speaking it is the range of one, with modulus m and residue a. Script capitals $(\mathscr{A}, \mathscr{B}, \dots)$ will be used to denote collections of arithmetic progressions, and $P(\mathscr{A})$ will denote the lowest common multiple of the moduli of the arithmetic progressions occurring in $\mathscr{A}$. As usual $\mathbb{Z}$ is the set of integers, (a, b) is the greatest common divisor of a and b, $[a, b]$ is the closed interval from a to b, and $\log_m x$ is the logarithm of x to the base m. The floor and ceiling functions $\lfloor x \rfloor$, and $\lceil x \rceil$ have their usual meanings, $a|b$ means a divides b and if p is a prime then $p^\alpha \parallel b$ means $p^\alpha | b$ but $p^{\alpha+1} \nmid b$.

In 1958, Stein [12] conjectured that if $\mathscr{A}$ is a collection of n pairwise disjoint arithmetic progressions with distinct moduli which does not cover $\mathbb{Z}$, then there is at least one integer in the interval $[1, 2^n]$ which does not belong to $\bigcup \mathscr{A}$. In 1962 Erdös [3] showed that this conjecture would hold if 2^n were replaced with $n2^n$, and

https://doi.org/10.1017/S1446788700000975 Published online by Cambridge University Press

made the stronger conjecture that if $\mathscr{A}$ is a collection of n arithmetic progressions, not necessarily disjoint or with distinct moduli, such that $\bigcup \mathscr{A} \supseteq [1, 2^n]$ then $\bigcup \mathscr{A} \supseteq \mathbb{Z}$. A proof of this conjecture was announced by Selfridge [9] at a meeting of the American Mathematical Society, although apparently not published. A proof was published by Crittenden and Vanden Eynden [1] in 1970 who in turn made the following conjecture [2]:

CONJECTURE. *If $\mathscr{A}$ is a collection of n arithmetic progressions, each with modulus $\geq k$, such that $\bigcup \mathscr{A} \supseteq [1, k2^{n-k+1}]$, then $\bigcup \mathscr{A} \supseteq \mathbb{Z}$.*

The conjecture has since been published by Guy [4] and Porubsky [7]. Note that the cases $k = 1$ and $k = 2$ of this conjecture are the same, and are equivalent to the Erdös conjecture proven by Crittenden and Vanden Eynden. Note also that the conjecture would not hold if $[1, k2^{n-k+1}]$ were replaced by any shorter interval, for the collection

$$\mathscr{A} = \{S(k, i) : i = 1, \dots, k-1\} \cup \{S(2^i k, 2^{i-1} k) : i = 1, \dots, n-k+1\}$$

covers the interval $[1, k2^{n-k+1} - 1]$ but does not cover $\mathbb{Z}$. Also observe that the interval $[1, k2^{n-k+1}]$ could be replaced by any interval of the form $[b+1, b+k2^{n-k+1}]$ without changing the truth or falsehood of the conjecture. This observation will allow us to simplify some of the proofs.

This paper is a contribution towards a proof of the conjecture. We show that if the conjecture fails for any k then a minimal counterexample (defined below) must possess certain characteristics, in particular that the value of n in the counterexample is bounded above by an explicit function of k. This means that to establish the conjecture for any value of k one needs only to check a finite number of cases, a process which has been done elsewhere [10] for the case $k = 3$. Unfortunately the 'finite number' increases exponentially with k.

We begin with several general results which will be applied to the conjecture in later sections.

Let P have prime factorisation

$$P = \prod\nolimits_{i=1}^{t} p_i^{\alpha_i}. \tag{1}$$

We define a function g by $g(P) = \sum_{i=1}^{t}((\alpha_i - 1)(p_i - 1) + 1)$.

THEOREM 1. *If $\mathscr{A}$ is such that $\bigcup \mathscr{A} \neq \mathbb{Z}$ and P is the least positive integer for which there exists an arithmetic progression $S(P, a)$ which is disjoint from $\bigcup \mathscr{A}$ then $|\mathscr{A}| \geq g(P)$.*

https://doi.org/10.1017/S1446788700000975 Published online by Cambridge University Press

PROOF. Without loss of generality we can assume $a = 0$. Let P have prime factorisation as in (1). We fix some i, and for convenience write α for α_i, p for p_i. For each of the $g(p^\alpha)$ ordered pairs (β, k) in the set

$$\{(\beta, k) : \beta \in [1, \alpha - 1],\ k \in [1, p - 1]\} \cup \{(\alpha - 1, 0)\} \tag{2}$$

we have, by the minimality of P,

$$\bigcup \mathscr{A} \cap (S(P/p^\alpha, 0) \cap S(p^\beta, kp^{\beta-1})) \neq \emptyset,$$

since the intersection of the two arithmetic progressions is an arithmetic progression with modulus less than P. Thus for each ordered pair (β, k), $\mathscr{A}$ contains an arithmetic progression, say $S(p^\gamma D, A)$ with $p \nmid D$, such that

$$S(p^\gamma D, A) \cap S(P/p^\alpha, 0) \cap S(p^\beta, kp^{\beta-1}) \neq \emptyset. \tag{3}$$

The Chinese Remainder Theorem implies that

$$A \equiv 0 \pmod{(D, P/p^\alpha)} \tag{4}$$

and

$$A \equiv kp^{\beta-1} \pmod{(p^\gamma, p^\beta)}. \tag{5}$$

$S(P, 0)$ is disjoint from this arithmetic progression so we have

$$A \not\equiv 0 \pmod{(p^\gamma D, P)}.$$

Now $S((p^\gamma D, P), 0)$ is the intersection of $S((p^\gamma, p^\alpha), 0)$, and $S((D, P/p^\alpha), 0)$, so A cannot belong to both of these. However, we know by (4) that it does belong to the second, so we conclude

$$A \not\equiv 0 \pmod{(p^\gamma, p^\alpha)}. \tag{6}$$

With (5) this implies that $\gamma \geq \beta$, so that $S(p^\gamma D, A)$ has the form

$$S(D, m(D, P/p^\alpha)) \cap S(p^\gamma, kp^{\beta-1} + np^\beta) \tag{7}$$

for some m and n, and with $\gamma \geq \beta$. We get such an arithmetic progression for each pair (β, k) allowed be (2) and since each is a subset of $S(p^\beta, kp^{\beta-1})$ for the corresponding pair (β, k) they are disjoint.

Thus we have $g(p_i^{\alpha_i})$ arithmetic progressions in $\mathscr{A}$ satisfying (7) for each prime in the set $\{p_1, p_2, \ldots, p_t\}$. This gives a total of $g(P)$ arithmetic progressions. Our final

https://doi.org/10.1017/S1446788700000975 Published online by Cambridge University Press

step is to show that arithmetic progressions of the form in (7) but corresponding to different values of p_i are distinct.

Suppose not. Then there is an arithmetic progression in $\mathscr{A}$, $S(p_i^\gamma D, A)$ say, with $p_i \nmid D$, which by (3) satisfies $S(p_i^\gamma D, A) \cap S(P/p_i^{\alpha_i}, 0) \neq \emptyset$ for some prime p_i, and for some prime p_j distinct from p_i satisfies $S(p_i^\gamma D, A) \cap S(P/p_j^{\alpha_j}, 0) \neq \emptyset$. But it is also clear that $S(P/p_i^{\alpha_i}, 0) \cap S(P/p_j^{\alpha_j}, 0) \neq \emptyset$, so we have three arithmetic progressions which intersect in pairs. Under such circumstances the three will have a non-empty intersection (see, for instance, [5, Theorem 3.16]) so that $S(p_i^\gamma D, A)$ intersects

$$S(P/p_i^{\alpha_i}, 0) \cap S(P/p_j^{\alpha_j}, 0) = S(P, 0),$$

contrary to the assumptions of the theorem. This shows that arithmetic progressions associated with different primes p_i are distinct. Arithmetic progressions corresponding to the same p_i are disjoint (and therefore distinct) by the remarks following display (7). Thus $\mathscr{A}$ contains $g(P)$ arithmetic progressions.

The bound in this theorem can be attained for any P, for instance by using the collection

$$\left\{S(p_i^\beta, kp_i^{\beta-1}) : \beta \in [1, \alpha_i - 1],\ k \in [1, p_i - 1]\right\} \cup \left\{S(p_i^{\alpha_i}, p_i^{\alpha_i - 1}),\ i = 1, \dots, t\right\}.$$

The next definition and theorem give a technique which is often used in work on problems concerned with covering the integers by arithmetic progressions.

Suppose we have a collection $\mathscr{A} = \{S(d_i, a_i) : i = 1, \dots, s, \dots, t\}$ where $s \leq t$, and an arithmetic progression $S(D, A)$, and suppose that $S(D, A)$ intersects $S(d_i, a_i)$ for $i = 1, \dots, s$, and not for i greater than s. For $i = 1, \dots, s$ we set $\delta_i = (D, d_i)$ and form another collection $\mathscr{A}^* = \{S(d_i^*, a_i^*) : i = 1, \dots, s\}$ where

$$d_i^* = d_i/\delta_i \tag{8}$$

and

$$a_i^* D/\delta_i \equiv (a_i - A)/\delta_i \pmod{d_i^*}. \tag{9}$$

We call $\mathscr{A}^*$ the *reduction of* $\mathscr{A}$ *via* $S(D, A)$ and $S(d_i^*, a_i^*)$ the *reduction of* $S(d_i, a_i)$ *via* $S(D, A)$.

Note that δ_i divides $a_i - A$ and that D/δ_i and d_i^* are relatively prime, so a_i^* is uniquely defined modulo d_i^*.

THEOREM 2. *Let $S(d^*, a^*)$ be the reduction of $S(d, a)$ via $S(D, A)$ and n be any integer. Then $A + nD \in S(d, a)$ if and only if $n \in S(d^*, a^*)$.*

https://doi.org/10.1017/S1446788700000975 Published online by Cambridge University Press

PROOF. Set $\delta = (D, d)$, so that we have $A \equiv a \pmod{\delta}$ and

$$a^* D/\delta \equiv (a - A)/\delta \pmod{d/\delta}.$$

Now $A + nD \in S(d, a)$ if and only if

$$\begin{aligned} nD &\equiv a - A \pmod{d} \\ \text{if and only if } nD/\delta &\equiv (a - A)/\delta \pmod{d/\delta} \\ \text{if and only if } n &\equiv a^* \pmod{d/\delta} \\ \text{if and only if } n &\in S(d^*, a^*). \end{aligned}$$

COROLLARY 1. *If $\mathscr{A}^*$ is the reduction of a collection $\mathscr{A}$ via $S(D, A)$, then $\bigcup \mathscr{A}$ includes $\{A + iD : i = 0, \dots, n - 1\}$ if and only if $\bigcup \mathscr{A}^*$ includes $\{0, \dots, n - 1\}$.*

PROOF. Immediate from the theorem.

A disadvantage of the reduction technique is that, in general, the modulus of an arithmetic progression is decreased when it is reduced. This may mean that an arithmetic progression with modulus greater than k turns into one with modulus less than k which makes it ineligible for inclusion in a counterexample. We now introduce another technique which has some of the properties of the reduction technique, but which does not change the moduli of the arithmetic progressions. We call this transformation T_p, where p is prime.

Let p be any prime and let $S(p^\alpha d, a)$ be an arithmetic progression in which $p \nmid d$. We define T_p by $T_p(S(p^\alpha d, a)) = S(p^\alpha d, b)$ where

$$\begin{aligned} b &\equiv a \pmod{p^\alpha} \\ pb &\equiv a \pmod{d}. \end{aligned} \tag{10}$$

Similarly we define a transformation on a collection $\mathscr{A}$ of arithmetic progressions: $T_p(\mathscr{A}) = \{T_p(S(d, a)) : S(d, a) \in \mathscr{A}\}$.

THEOREM 3. *Let p be a prime and let $\mathscr{A}$ be a collection of arithmetic progressions. Then $\bigcup \mathscr{A} = \mathbb{Z}$ if and only if $\bigcup T_p(\mathscr{A}) = \mathbb{Z}$.*

PROOF. Let $P(\mathscr{A}) = p^\alpha P$ where $p \nmid P$. Let m be any integer, and find another integer n such that

$$\begin{aligned} n &\equiv m \pmod{p^\alpha} \\ pn &\equiv m \pmod{P}. \end{aligned} \tag{11}$$

https://doi.org/10.1017/S1446788700000975 Published online by Cambridge University Press

We will show that m belongs to an arithmetic progression $S(p^\alpha d, a)$ if and only if n belongs to $T_p(p^\alpha d, a)$, where p does not divide d.

$$\begin{aligned} &m \in S(p^\alpha d, a) \\ &\text{if and only if } m \equiv a \pmod{p^\alpha} \text{ and } m \equiv a \pmod{d} \\ &\text{if and only if } n \equiv a \pmod{p^\alpha} \text{ and } pn \equiv a \pmod{d} \\ &\text{if and only if } n \in T_p(S(p^\alpha d, a)) \end{aligned}$$

Since (11) describes a bijection from $\mathbb{Z}_{P(\mathscr{A})}$ to itself, it follows that each integer belongs to an arithmetic progression in $\mathscr{A}$ if and only if each integer belongs to an arithmetic progression in $T_p(\mathscr{A})$.

THEOREM 4. *If $S(p^\alpha d, a)$ is an arithmetic progression, $p \nmid d$ and $\theta > \alpha \geq 0$, then $mp^\theta \in S(p^\alpha d, a)$ if and only if $mp^{\theta-1} \in T_p(S(p^\alpha d, a))$.*

PROOF. Let $T_p(S(p^\alpha d, a)) = S(p^\alpha d, b)$. Then by (10), $mp^\theta \equiv a \pmod{d}$ if and only if $mp^{\theta-1} \equiv b \pmod{d}$.

Also by (10) and the hypothesis that $\theta > \alpha$, $mp^\theta \equiv a \pmod{p^\alpha}$ if and only if $mp^{\theta-1} \equiv b \pmod{p^\alpha}$. The theorem then follows.

2. Characterisation of a counterexample

For a given integer $k \geq 3$ we define a *minimal counterexample* for this k to be a collection $\mathscr{A}$ of n arithmetic progressions, each with modulus at least k, and such that $\bigcup \mathscr{A} \supseteq [1, k2^{n-k+1}]$ and $\bigcup \mathscr{A} \neq \mathbb{Z}$, and further such that

(a) n is the least integer for which such an $\mathscr{A}$ exists, and

(b) in any other collection of n arithmetic progressions having these properties, the sum of the moduli of the arithmetic progressions is at least equal to the sum of the moduli of the arithmetic progressions appearing in $\mathscr{A}$.

This section will be concerned with obtaining constraints on the moduli of the arithmetic progressions in a minimal counterexample.

In obtaining necessary conditions for $\mathscr{A}$ to be a minimal counterexample we will often use proof by contradiction, showing that if $\mathscr{A}$ did not possess the specified property then it would be possible to construct another counterexample with lower cardinality, or with the same cardinality and the size of one or more of the moduli reduced. In the proofs we sometimes assume that a minimal counterexample $\mathscr{A}$ does not cover 0. This involves no loss of generality.

THEOREM 5. *If $\mathscr{A}$ is a minimal counterexample which does not cover* 0, *and $S(bc, a)$ belongs to $\mathscr{A}$ with $b \geq k$, $c > 1$, then*

https://doi.org/10.1017/S1446788700000975 Published online by Cambridge University Press

(a) $\bigcup\mathscr{A} \supseteq \mathbb{Z}\backslash S(b, 0)$,
(b) $a \equiv 0 \pmod{b}$,
(c) $S(bc, a) \subseteq S(b, 0)$.

PROOF. Write $\mathscr{A} = \mathscr{A}^* \cup \{S(bc, a)\}$. Now $S(b, a) \supset S(bc, a)$, so $(\bigcup\mathscr{A}^*) \cup S(b, a) \supseteq \bigcup\mathscr{A} \supseteq [1, k2^{n-k+1}]$.

This means that $\mathscr{A}^* \cup \{S(b, a)\}$ is a counterexample to the conjecture, contradicting the minimality of $\mathscr{A}$, unless

$$(12) \qquad \left(\bigcup\mathscr{A}^*\right) \cup S(b, a) = \mathbb{Z},$$

so we conclude that this is so. We assumed that $\mathscr{A}$, and therefore $\mathscr{A}^*$, does not cover 0, so 0 must belong to $S(b, a)$. That is, $a \equiv 0 \pmod{b}$. This is part (b) of the theorem. Part (a) then follows from (12), and part (c) from part (b).

COROLLARY 2. *Suppose $\mathscr{A}$ is a minimal counterexample that does not cover* 0, *and that $S(d, a)$ is an element of $\mathscr{A}$.*

(a) *If $2^\alpha \| d$ and $2^\alpha \geq k$ then $d = 2^\alpha$.*
(b) *If p is an odd prime, $p^{\alpha+1} \| d$ and $p^\alpha \geq k$ then $d = p^{\alpha+1}$.*

PROOF. (a) Suppose $d = 2^\alpha d_0$ where d_0 is odd and greater than 1. Then by part (b) of Theorem 5 we have

$$(13) \qquad a \equiv 0 \pmod{2^\alpha}.$$

Since $2^{\alpha-1}d_0 > 2^\alpha \geq k$, part (b) also implies that

$$(14) \qquad a \equiv 0 \pmod{2^{\alpha-1}d_0}.$$

Together (13) and (14) imply that

$$a \equiv 0 \pmod{2^\alpha d_0}$$

which implies $\mathscr{A}$ covers 0, a contradiction.

(b) Suppose $d = p^{\alpha+1}d_0$ where $d_0 > 1$ and p is an odd prime which does not divide d_0. We again apply part (b) of Theorem 5 twice, first with $p^{\alpha+1}$ in the role of b and second with $p^\alpha d_0$ in that role, obtaining a contradiction as in part (a).

Note that Theorem 5 does not enable us to forbid all arithmetic progressions with modulus $p^\alpha d_0$ with $p^\alpha \geq k$ and $d_0 > 1$. If d_0 is a prime or prime power with $d_0 p^{\alpha-1} < k$ we cannot obtain a contradiction as in the proof of the corollary. The next few results

https://doi.org/10.1017/S1446788700000975 Published online by Cambridge University Press

do give an improvement in the case of primes which are at least k. For these we need the following definition.

An *irredundant covering system* is a collection of arithmetic progressions $\mathscr{A}$ such that $\bigcup \mathscr{A} = \mathbb{Z}$ and such that no proper subcollection of $\mathscr{A}$ has this property. Such collections are also sometimes called *regular covering systems* or just *covering systems*. We use two properties of such systems, the first of which is proved in [11].

THEOREM 6. *If $\mathscr{A} = \{S(d_i, a_i) : i = 1, \dots, t\}$ is an irredundant covering system, and p is a prime dividing $P(\mathscr{A})$, then the set $\{a_i : p \mid d_i\}$ contains a complete residue system modulo p.*

THEOREM 7. *If $\mathscr{A}$ is a minimal counterexample and p is a prime greater than or equal to k, then for all integers b we have $\bigcup \mathscr{A} \not\supseteq \mathbb{Z} \setminus S(p, b)$.*

PROOF. Suppose otherwise, so that $\mathscr{A} \cup \{S(p, b)\}$ covers the integers and any irredundant subcovering of it must contain $S(p, b)$. By Theorem 6, $\mathscr{A}$ therefore contains at least $p - 1$ arithmetic progressions whose moduli are divisible by p and which are disjoint from $S(p, b)$.

We now reduce the collection $\{S(d, a) \in \mathscr{A} : S(d, a) \cap S(p, b) \neq \emptyset\}$ via $S(p, b)$, to obtain a collection $\mathscr{A}^*$ with

$$|\mathscr{A}^*| \leq n - p + 1. \tag{15}$$

Now $\mathscr{A}$ being a counterexample implies

$$\bigcup \mathscr{A} \supseteq [1, k2^{n-k+1}] \cap S(p, b) = \{b + ip : i = 0, \dots, [k2^{n-k+1}/p] - 1\}.$$

Here we have assumed, as we may, that $1 \leq b \leq p$. By Theorem 2 we then have

$$\bigcup(\mathscr{A}^*) \supseteq [0, \lfloor k2^{n-k+1} \rfloor - 1]. \tag{16}$$

Also, since $\bigcup \mathscr{A} \supseteq \mathbb{Z} \setminus S(p, b)$, $\bigcup \mathscr{A} \neq \mathbb{Z}$, we have $\bigcup \mathscr{A} \not\supseteq S(p, b)$. Again by Theorem 2 we therefore have $\bigcup \mathscr{A}^* \neq \mathbb{Z}$.

Using the $k = 1$ version of the conjecture (which is the case proven by Crittenden and Vanden Eynden) and equation (16) we have $[k2^{n-k+1}/p] < 2^{n-p+1}$ which leads to $p - \log_2 p < k - \log_2 k$. This is impossible since the function $x - \log_2 x$ increases with x for $x > 2$ and we have $p \geq k > 2$. This contradiction proves the theorem.

COROLLARY 3. *Suppose $\mathscr{A}$ is a minimal counterexample, p is a prime at least k and $S(pd, a)$ belongs to $\mathscr{A}$. Then $d = 1$.*

PROOF. Suppose that $d \neq 1$. We may form another minimal counterexample $\mathscr{A}^*$ which does not cover 0 and whose elements have the same moduli as the corresponding elements of $\mathscr{A}$. Then by part (a) of Theorem 5 we have $\bigcup \mathscr{A}^* \supseteq \mathbb{Z} \backslash S(p, 0)$ which contradicts Theorem 7.

This corollary gives the first important constraint on the moduli appearing in a minimal counterexample. We have shown that each such modulus is either a prime at least k or a product of primes less than k. The corollary to the next theorem will provide a further constraint on the arithmetic progressions with prime modulus. We first remark that any arithmetic progression with modulus d is the union of $\lceil k/d \rceil$ arithmetic progressions each with modulus at least k, since

$$S(d, a) = \bigcup_{i=1}^{\lceil k/d \rceil} S(\lceil k/d \rceil d, a + id)$$

and $\lceil k/d \rceil d \geq k$.

THEOREM 8. *If $\mathscr{A}$ is a minimal counterexample and $S(d_0, a_0)$ is an arithmetic progression such that $\bigcup \mathscr{A} \not\supseteq S(d_0, a_0)$ then*

$$\sum_{\substack{S(d,a) \in \mathscr{A},\ (d,d_0)>1, \\ a \equiv a_0 \pmod{(d,d_0)}}} \lceil k(d, d_0)/d \rceil + \log_2 d_0 > |\{S(d, a) \in \mathscr{A}(d, d_0) > 1\}|. \tag{17}$$

PROOF. We set

$$\begin{aligned} \mathscr{A}_1 &= \{S(d, a) \in \mathscr{A} : (d, d_0) > 1, \quad a \equiv a_0 \pmod{d, d_0}\}, \\ \mathscr{A}_2 &= \{S(d, a) \in \mathscr{A} : (d, d_0) > 1, \quad a \not\equiv a_0 \pmod{d, d_0}\}, \\ \mathscr{A}_3 &= \{S(d, a) \in \mathscr{A} : (d, d_0) = 1\} \quad \text{and} \quad |\mathscr{A}_i| = N_i \text{ for } i = 1, 2, 3. \end{aligned}$$

No arithmetic progression in $\mathscr{A}_2$ intersects $S(d_0, a_0)$ so

$$\bigcup (\mathscr{A}_1 \cup \mathscr{A}_3) \supseteq S(d_0, a_0) \cap [1, k2^{n-k+1}].$$

If we assume, as we may, that $1 \leq a_0 \leq d_0$ then we have

$$\bigcup (\mathscr{A}_1 \cup \mathscr{A}_3) \supseteq \{a_0 + id_0 : i = 0, \dots, [k2^{n-k+1} - a_0)/d_0]\}.$$

We now reduce $\mathscr{A}_1$ and $\mathscr{A}_3$ via $S(d_0, a_0)$ to get $\mathscr{A}_1^*$ and $\mathscr{A}_3^*$ so that by Corollary 1,

$$\bigcup (\mathscr{A}_1^* \cup \mathscr{A}_3^*) \supseteq [0, \lfloor k2^{n-k+1}/d_0 \rfloor - 1].$$

From this we see that

$$\bigcup \{S(\delta, a + 1) : S(\delta, a) \in \mathscr{A}_1^* \cup \mathscr{A}_3^*)\} \supseteq [1, \lfloor k2^{n-k+1}/d_0 \rfloor]. \tag{18}$$

https://doi.org/10.1017/S1446788700000975 Published online by Cambridge University Press

By Theorem 2 and our assumption that $\bigcup \mathscr{A}$ does not include $S(d_0, a_0)$ the collection in (18) does not cover the integers. It thus has some of the properties of a counterexample. However the reduction of an arithmetic progression $S(d, a)$ via $S(d_0, a_0)$ has modulus $d/(d, d_0)$ and in the case of those arithmetic progressions in $\mathscr{A}_1^*$ this may be less than k. To overcome this difficulty we replace each arithmetic progression that appears in the collection in (18) and that originated in $\mathscr{A}_1$ with $\lceil k(d, d_0)/d \rceil$ arithmetic progressions each having modulus at least k, as described in the remark preceding Theorem 8. We combine this collection with $\{S(d, a+1) : S(d, a) \in \mathscr{A}_3^*\}$ to form a new collection $\mathscr{B}$; $\bigcup \mathscr{B}$ is then identical to the left-hand side of (18), each modulus appearing in it is at least k and

$$(19) \qquad |\mathscr{B}| = \sum_{S(d,a) \in \mathscr{A}_1} \lceil k(d, d_0)/d \rceil + N_3 = N, \quad \text{say.}$$

By (18) and the remarks following it, we also have

$$(20) \qquad \bigcup \mathscr{B} \supseteq [1, \lfloor k2^{n-k+1}/d_0 \rfloor], \qquad \bigcup \mathscr{B} \neq \mathbb{Z}.$$

Now the sum in (19) is the sum that appeared in (17). If it is at least $N_1 + N_2$ we have already established inequality (17) since the right-hand side of that inequality is $N_1 + N_2$. We therefore assume it to be less than $N_1 + N_2$ so that $|\mathscr{B}| < N_1 + N_2 + N_3 = n$.

Since $\mathscr{A}$ is a minimal counterexample, we have $\lfloor k2^{n-k+1}/d_0 \rfloor < k2^{N-k+1}$. This leads to $N > n - \log_2 d_0$.

On substituting for N and n and recalling the definitions of $\mathscr{A}_1$ and $\mathscr{A}_2$ we obtain the required inequality.

COROLLARY 4. *If $\mathscr{A}$ is a minimal counterexample and p is a prime number, $p \geq k$, then the number of arithmetic progressions in $\mathscr{A}$ having modulus p is less than* $\log_2 p$.

PROOF. By Corollary 3 the only arithmetic progressions in $\mathscr{A}$ having modulus divisible by p have modulus equal to p. We can therefore choose a residue class modulo p, $S(p, a_0)$ say, which intersects no arithmetic progression in $\mathscr{A}$ with modulus divisible by p.

We now use $S(p, a_0)$ in the role of $S(d_0, a_0)$ in Theorem 8. By the preceding remark we see that the sum that appears in the statement of that theorem is empty. We then have

$$\begin{aligned} \log_2 p &> |\{S(d, a) \in \mathscr{A} : (d, p) > 1\}| \\ &= |\{S(d, a) \in \mathscr{A} : d = p\}|. \end{aligned}$$

The final results of this section concern those moduli which are divisible by primes less than k.

https://doi.org/10.1017/S1446788700000975 Published online by Cambridge University Press

THEOREM 9. *If $\mathscr{A}$ is a minimal counterexample which does not cover* 0, *p is a prime less than k and $\mathscr{A}$ includes a subcollection $\{S(p^\alpha, ip^{\alpha-1}) : i = 1, \dots, p-1\}$, then $\alpha = \lceil \log k/\log p \rceil$.*

PROOF. Notice that with $\beta = \lceil \log k/\log p \rceil$, the least power of p which is not less than k is p^β, so we must have

$$\alpha \geq \lceil \log k/\log p \rceil. \tag{21}$$

Suppose we have strict inequality in (21) and write $\mathscr{A} = \mathscr{A}_1 \cup \mathscr{A}_2 \cup \mathscr{A}_3$ where

$$\begin{aligned} \mathscr{A}_1 &= \{S(d,a) \in \mathscr{A} : p^{\alpha+1} \mid d\}, \\ \mathscr{A}_2 &= \{S(d,a) \in \mathscr{A} : p^{\alpha} \parallel d\}, \\ \mathscr{A}_3 &= \{S(d,a) \in \mathscr{A} : p^{\alpha} \nmid d\}. \end{aligned}$$

Now by hypothesis $|\mathscr{A}_2| \geq p - 1$, and by our supposition $p^{\alpha-1} \geq k$.

Corollary 2 and Theorem 5 then imply that any arithmetic progression in $\mathscr{A}_2$ has the form $S(p^\alpha, ip^{\alpha-1})$ and that $\bigcup \mathscr{A} \supseteq \mathbb{Z}\backslash S(p^{\alpha-1}, 0)$.

Since $\mathscr{A}$ does not cover 0, $\mathscr{A}_2$ does not contain $S(p^\alpha, 0)$ so $\bigcup \mathscr{A}_2 \subseteq S(p^{\alpha-1}, 0)\backslash S(p^\alpha, 0)$.

Similarly we have $\cup \mathscr{A}_1 \subseteq S(p^\alpha, 0)$.

These last three inclusions imply $\bigcup \mathscr{A}_3 \cup S(p^{\alpha-1}, 0) = \mathbb{Z}$.

We now use the transformation T_p introduced in the first section. By Theorem 3 the above display implies

$$\bigcup T_p(\mathscr{A}_3) \cup T_p(S(p^{\alpha-1}, 0)) = \mathbb{Z}.$$

Since $S(p^{\alpha-1}, 0)$ is not changed by T_p, this is equivalent to

$$\bigcup T_p(\mathscr{A}_3) \supseteq \mathbb{Z}\backslash S(p^{\alpha-1}, 0). \tag{22}$$

We now turn our attention to the collection $\mathscr{A}_1$. If $S(d, a)$ is an element of this then by its definition and Corollary 5 both a and d are divisible by p. We form another collection $\mathscr{A}_1^* = \{S(d/p, a/p) : S(d,a) \in \mathscr{A}_1\}$ and note that each modulus appearing in $\mathscr{A}_1^*$ is at least p^α which is at least k.

Since we have shown that $\bigcup \mathscr{A}_2$ is disjoint from $S(p^\alpha, 0)$ we have

$$\begin{aligned} \bigcup(\mathscr{A}_1 \cup \mathscr{A}_3) &\supseteq S(p^\alpha, 0) \cap [1, k2^{n-k+1}] \\ &= \{ip^\alpha : i = 1, \dots, \lfloor k2^{n-k+1}/p^\alpha \rfloor\}. \end{aligned}$$

Now ip^α belongs to an arithmetic progression in $\mathscr{A}_1$ if and only if $ip^{\alpha-1}$ belongs to the corresponding arithmetic progression in $\mathscr{A}_1^*$. Also, by Theorem 4, ip^α belongs to

https://doi.org/10.1017/S1446788700000975 Published online by Cambridge University Press

an arithmetic progression in $\mathscr{A}_3$ if and only if $ip^{\alpha-1}$ belongs to the equivalent arithmetic progression in $T_p(\mathscr{A}_3)$. Thus

$$\begin{aligned}&\bigcup(\mathscr{A}_1^* \cup T_p(\mathscr{A}_3)) \supseteq \{ip^{\alpha-1} : i = 1, \dots, \lfloor k2^{n-k+1}/p^\alpha \rfloor\},\\ &\bigcup(\mathscr{A}_1^* \cup T_p(\mathscr{A}_3)) \not\supseteq \{0\}.\end{aligned}$$

Since by (22) the collection $\mathscr{A}_1^* \cup T_p(\mathscr{A}_3)$ covers all integers which are not divisible by $p^{\alpha-1}$, the least positive integer not covered by the collection is at least

$$\lfloor k2^{n-k+1}/p^\alpha \rfloor p^{\alpha-1} + p^{\alpha-1} > \lfloor k2^{n-k+1}/p \rfloor.$$

We therefore have

$$\begin{aligned}&\bigcup(\mathscr{A}_1^* \cup T_p(\mathscr{A}_3)) \supseteq [1, \lfloor k2^{n-k+1}/p \rfloor],\\ &\bigcup(\mathscr{A}_1^* \cup T_p(\mathscr{A}_3)) \neq \mathbb{Z},\\ &|\mathscr{A}_1^* \cup T_p(\mathscr{A}_3)| \le n - p + 1,\end{aligned}$$

and each arithmetic progression in the collection has modulus at least k. Since $\mathscr{A}$ was assumed minimal we must have $\lfloor k2^{n-k+1}/p \rfloor < k2^{n-p-k+2}$ which leads to $2^p < 2p$, which is impossible for $p \ge 2$. This contradiction proves the theorem.

COROLLARY 5. *Suppose that $\mathscr{A}$ is a minimal counterexample that does not cover* 0.
(a) *The highest power of* 2 *dividing $P(\mathscr{A})$ is at most $2^{\lceil \log_2 k \rceil}$.*
(b) *If p is an odd prime less than k, the highest power of p dividing $P(\mathscr{A})$ is at most $p^{\lceil \log_p k \rceil + 1}$.*

PROOF. (a) Let 2^α be the highest power of 2 dividing $P(\mathscr{A})$. Then $\mathscr{A}$ contains an arithmetic progression of the form $S(2^\alpha d, a)$. If $2^\alpha < k$ we are done, and if $2^\alpha \ge k$ we have, by Theorem 5 and Corollary 2, $S(2^\alpha d, a) = S(2^\alpha, 2^{\alpha-1})$.

By Theorem 9 we then have $\alpha = \lceil \log k / \log 2 \rceil$ as required.

(b) We prove this part by contradiction. Suppose that $p^{\alpha+1}$ is the highest power pf p dividing $P(\mathscr{A})$ and that

$$\alpha > \lceil \log k / \log p \rceil. \tag{23}$$

Then $\mathscr{A}$ contains an arithmetic progression of the form $S(p^{\alpha+1}d, a)$. By Theorem 5, part (a), we have $\bigcup \mathscr{A} \supseteq \mathbb{Z} \backslash S(p^\alpha, 0)$. Thus $\bigcup \mathscr{A}$ covers $S(p^\alpha, ip^{\alpha-1})$ for $i = 1, \dots, p-1$ but does not cover $S(p^\alpha, 0)$. For this to occur $\mathscr{A}$ must contain $p - 1$ arithmetic progressions of the form $S(p^\alpha d_i, a_i)$ with

$$a_i \equiv ip^{\alpha-1} \pmod{p^\alpha} \quad \text{for } i = 1, \dots, p-1.$$

https://doi.org/10.1017/S1446788700000975 Published online by Cambridge University Press

By Theorem 5 each d_i equals 1, so these arithmetic progressions are precisely

$$\{S(p^\alpha, ip^{\alpha-1}) : i = 1, \dots, p-1\}.$$

But now Theorem 9 says that α equals $\lceil \log k/\log p \rceil$, contradicting (23).

3. A sieve for the problem

In this section we are concerned with arithmetic progressions having prime modulus $\geq k$, and derive an upper bound on the length of an interval that can be covered by n such arithmetic progressions. In the next section we apply this result to the conjecture. We begin with some notation.

Throughout this section $\mathscr{A}$ is a collection of arithmetic progressions, each with prime modulus, and k a positive integer ≥ 3. For each prime p set

$$c(p) = |\{S(d,a) \in \mathscr{A} : d = p\}|.$$

The collection $\mathscr{A}$ also satisfies the following conditions

$$|\mathscr{A}| = n, \tag{24}$$

$$c(p) = 0 \quad \text{if} \quad p < k, \tag{25}$$

$$c(p) \leq \lfloor \log_2 p \rfloor \quad \text{otherwise}. \tag{26}$$

The section's first theorem gives some lower bounds on the number of positive integers $\leq N$ which do not belong to $\cup\mathscr{A}$. It is similar to Lemma 2 of [1].

THEOREM 10. *With the above notation, let $\{p_1, p_2, \dots, p_t\}$ be the set of primes for which $c(p) \neq 0$, and write c_i for $c(p_i)$. Let N be any positive integer and let s be an integer satisfying $1 \leq s \leq t$.*

(a) $$\left|\left\{m : 1 \leq m \leq N,\ m \notin \bigcup \mathscr{A}\right\}\right|$$
$$> N\left(1 - \sum_{i=s}^{t} c_i/p_i\right)\prod_{i=1}^{s-1}(1 - c_i/p_i) - \left(1 + \sum_{i=s}^{t} c_i\right)\prod_{i=1}^{s-1}(1 + c_i).$$

(b) $$\left|\left\{m : 1 \leq m \leq N,\ m \notin \bigcup \mathscr{A}\right\}\right|$$
$$\geq N - c_1(\lfloor N/p_1 \rfloor + 1) - \sum_{i=2}^{t} c_i(\lfloor N/p_i \rfloor - c_1\lfloor N/p_1p_i \rfloor + 1).$$

(c) $$\left|\left\{m : 1 \leq m \leq N,\ m \notin \bigcup \mathscr{A}\right\}\right|$$
$$\geq N - \sum_{i=1}^{t} c_i(\lfloor N/p_i \rfloor + 1) + c_1c_2\lfloor N/p_1p_2 \rfloor$$
$$+ \sum_{i=3}^{t} c_i(c_1\lfloor N/p_1p_i \rfloor + c_2\lfloor N/p_2p_i \rfloor - c_1c_2(\lfloor N/p_1p_2p_i \rfloor + 1)).$$

https://doi.org/10.1017/S1446788700000975 Published online by Cambridge University Press

PROOF. We shall use $\sum'$ to denote a sum in which at most one of the subscripts is $\geq s$ and all allowable subscripts are covered. Note that, with this notation, for any $x_1, x_2, \ldots, x_t$,

(27)
$$1 + \sum{}' x_i + \sum{}' x_i x_j + \cdots + \sum{}' x_{i_1} x_{i_2} \cdots x_{i_s} = \left(1 + \sum_{i=s}^{t} x_i\right) \prod_{i=1}^{s-1} (1 + x_i).$$

For $i = 1, 2, \ldots, t$ we let S_i denote the union of those arithmetic progressions in $\mathscr{A}$ which have modulus p_i. From the Chinese Remainder Theorem each set of $p_{i_1} p_{i_2} \cdots p_{i_r}$ consecutive integers contains exactly $c_{i_1} c_{i_2} \cdots c_{i_r}$ elements of $S_{i_1} \cap S_{i_2} \cap \cdots \cap S_{i_r}$ and hence

$$(28) \qquad |S_{i_1} \cap S_{i_2} \cap \cdots \cap S_{i_r} \cap [1, N]| = \lfloor N / \prod_{j=1}^{r} p_{i_j} \rfloor \prod_{j=1}^{r} c_{i_j} + E \prod_{j=1}^{r} c_{i_j}$$

where E satisfies $0 \leq E \leq 1$. It follows that

$$(29) \qquad |S_{i_1} \cap S_{i_2} \cap \cdots \cap S_{i_r} \cap [1, N]| = N \prod_{j=1}^{r} c_{i_j} / p_{i_j} + E' \prod_{j=1}^{r} c_{i_j}$$

where E' satisfies $-1 < E' < 1$.

We denote the characteristic function of a set A by χ_A. With this notation

$$\begin{aligned} \chi_{\mathbb{Z} \setminus \cup \mathscr{A}} &= \prod_{i=s}^{t} (1 - \chi_{S_i}) \prod_{i=1}^{s-1} (1 - \chi_{S_i}) \\ &\geq \left(1 - \sum_{i=s}^{t} \chi_{S_i}\right) \prod_{i=1}^{s-1} (1 - \chi_{S_i}). \end{aligned}$$

Using identity (27) with $-\chi_{S_i}$ in the role of x_i we obtain

$$\chi_{\mathbb{Z} \setminus \cup \mathscr{A}} \geq 1 - \sum_i{}' \chi_{S_i} + \sum_{i,j}{}' \chi_{S_i} \chi_{S_j} - \cdots .$$

Using the fact that for any sets A and B we have $\chi_{A \cap B} = \chi_A \chi_B$ we obtain

$$(30) \qquad \begin{aligned} \left| \left\{ m : 1 \leq m \leq N, m \notin \bigcup \mathscr{A} \right\} \right| &= \sum_{m=1}^{N} \chi_{\mathbb{Z} \setminus \cup \mathscr{A}}(m) \\ &\geq N - \sum_i{}' |S_i \cap [1, N]| + \sum_{i,j}{}' |S_i \cap S_j \cap [1, N]| - \cdots . \end{aligned}$$

https://doi.org/10.1017/S1446788700000975 Published online by Cambridge University Press

Using equation (29) we see that the right-hand side of (30) is greater than

$$N - {\sum_i}' \left(N\frac{c_i}{p_i} + c_i \right) + {\sum_{i,j}}' \left(N\frac{c_i c_j}{p_i p_j} - c_i c_j \right) - \cdots .$$

We now collect those terms involving N and those not involving N, apply identity (27) to each collection of terms, and obtain part (a) of the theorem.

To obtain part (b), we set $s = 1$. Using (30) and (28), we obtain

$$\left| \left\{ m : 1 \le m \le N,\ m \notin \bigcup \mathscr{A} \right\} \right| \ge N - \sum_{i=1}^{t} (c_i \lfloor N/p_i \rfloor + c_i) + \sum_{i=2}^{t} c_1 c_i (\lfloor N/p_1 p_i \rfloor),$$

and the right-hand side simplifies to the right-hand side of part (b).

Part (c) is obtained in the same way as part (b) after setting $s = 2$.

Parts (b) and (c) of this theorem are used in the next section. We use part (a) to derive a corollary, but first we need some more notation: we set

$$M(\mathscr{A}) = \max \left\{ N : \bigcup \mathscr{A} \supseteq [1, N] \right\}.$$

If $\bigcup \mathscr{A}$ does not include 1, we set $M(\mathscr{A}) = 0$.

COROLLARY 6. *Let p_0 be a modulus appearing in $\mathscr{A}$ such that $1 - \sum_{p \ge p_0} c(p)/p > 0$. (This will hold for sufficiently large p_0 since the number of non-zero $c(p)$'s is finite.) Then*

$$M(\mathscr{A}) < \frac{1 + \sum_{p \ge p_0} c(p)}{1 - \sum_{p \ge p_0} c(p)/p} \prod_{p < p_0} \frac{1 + c(p)}{1 - c(p)/p}. \tag{31}$$

PROOF. By the definition of $M(\mathscr{A})$ we have

$$\left| \left\{ m : 1 \le m \le M(\mathscr{A}),\ m \notin \bigcup \mathscr{A} \right\} \right| = 0.$$

Thus we may use part (a) of the theorem with 0 replacing the left-hand side of the inequality and $M(\mathscr{A})$ replacing N on the right and p_0 in the role of p_s. An easy rearrangement then gives (31).

The rest of this section is devoted to getting upper bounds for $M(\mathscr{A})$. This requires getting an upper bound for the right-hand side of (31) which is independent of the values of the variables $c(p)$. To do this we need yet more notation.

https://doi.org/10.1017/S1446788700000975 Published online by Cambridge University Press

We set :

p is an odd prime,
p' is the prime preceding p,
x is a positive real number,

$$A(x) = \prod_{p<x} \frac{p}{p-1}, \qquad W(p) = p' - \lfloor \log_2 p' \rfloor, \qquad V(x, p) = \frac{1+x}{1-x/p} 2^{-x},$$

and $r(k, n)$ is the least prime r such that

$$r - 1 + \sum_{k \le p < r} \lfloor \log_2 p \rfloor \ge n.$$

We notice that the left-hand side here increases with r and so the function is well defined.

LEMMA 1. *For $p \ge 7$ we have $p - 4 \ge W(p) > 2$.*

PROOF. For such p, $\lfloor \log_2 p' \rfloor \ge 2$ and so $W(p) \le p' - 2 \le p - 4$. Also, for $p' \ge 5$ we have $\log_2 p' < p'/2$ and so $W(p) > p'/2 > 2$.

THEOREM 11. *For fixed $p \ge 7$ the function $V(x, p)$ is strictly decreasing as a function of x in the interval* $[1, p-2]$.

PROOF. We write $f(x) = V(x, p)$. Then $f(x) > 0$ in the interval $[1, p-2]$ and by logarithmic differentiation we have

$$\begin{aligned} \frac{f'(x)}{f(x)} &= \frac{p+1}{(1+x)(p-x)} - \log 2 \\ &\le \frac{p+1}{2(p-1)} - \log 2, \end{aligned}$$

since the minimum of $(1+x)(p-x)$ on $[1, p-2]$ occurs at one of the end points. For $p \ge 7$ we have

$$\frac{p+1}{2(p-1)} \le \frac{2}{3} < \log 2$$

and since $f(x) > 0$ it follows that $f'(x) < 0$. Thus $f(x)$ is strictly decreasing on $[1, p-2]$.

COROLLARY 7. *If m is an integer satisfying $0 \le m \le \lfloor \log_2 p \rfloor$, then*

$$V(m, p) \le p/(p-1). \tag{32}$$

https://doi.org/10.1017/S1446788700000975 Published online by Cambridge University Press

PROOF. It is easy to check that this holds for $p = 2, 3, 5$ and whenever $m = 0$. For $p \geq 7$ we use Theorem 11, which says that $V(m, p)$ attains its maximum value in the interval $[1, p-2]$ when $m = 1$, and clearly $V(1, p) = p/(p-1)$.

COROLLARY 8. *The function $A(p)V(W(p), p)$ is strictly decreasing for $p \geq 5$.*

PROOF. It is easily checked that

$$A(7)V(W(7), 7) < A(5)V(W(5), 5).$$

and

$$A(11)V(W(11), 11) < A(7)V(W(7), 7).$$

We therefore assume $p \geq 11$ and let p^+ be the prime immediately succeeding p. Using Lemma 1 and the definition of W we then have

$$1 < W(P) + 1 \leq W(p^+) < p^+ - 2.$$

Applying Theorem 11 we then have

$$\begin{aligned} V(W(p^+), p^+) &\leq V(W(p) + 1, p^+) < V(W(p) + 1, p) \\ &= \frac{1}{2}\left(1 + \frac{1}{1 + W(p)}\right)\left(1 + \frac{1}{p - (W(p) + 1)}\right) V(W(p), p). \end{aligned}$$

Using the bounds on W(p) in Lemma 1 this is at most

$$\frac{1}{2}\left(1 + \frac{1}{3}\right)\left(1 + \frac{1}{3}\right) V(W(p), p) = \frac{8}{9} V(W(p), p) < \frac{p-1}{p} V(W(p), p),$$

for $p \geq 11$. Since $A(p^+) = p/(p-1)A(p)$ this establishes the corollary.

LEMMA 2. *If m is an integer, $m \geq 2$, we have $A(m) < 2 \log m$.*

PROOF. By direct calculation we find that the inequality holds for $m \leq 18$. For higher values we use the following known result (see [8, Theorem 8, Corollary 1]),

$$\prod_{p \leq m} \frac{p}{p-1} < e^{\gamma} \log m \left(1 + (\log m)^{-2}\right),$$

where γ is Euler's constant. This holds for all real m exceeding 1. If $m \geq 19$ then the right side is less than

$$1.79 \left(1 + (\log 19)^{-2}\right) \log m < 2 \log m.$$

https://doi.org/10.1017/S1446788700000975 Published online by Cambridge University Press

LEMMA 3. *With $r = r(k, n)$ as defined above, and with $r' = r'(k, n)$ being the prime preceding $r(k, n)$, we have for $k \geq 3$ and $n \geq 10$:*

(a) $r(k, n) > 2n/5$,
(b) $r'(k, n) > n/3$,
(c) $r(k, n) < 2n$.

PROOF. (a) It is sufficient to show that this holds for $k = 3$. To do this we show that if $r \leq 2n/5$ the inequality defining $r(3, n)$,

$$r - 1 + \sum_{3 \leq p < r} \lfloor \log_2 p \rfloor \geq n \tag{33}$$

does not hold. We note that

$$\begin{aligned} \sum_{3 \leq p < r} \lfloor \log_2 p \rfloor &< \sum_{p < r} \log_2 p - 1 \\ &\leq \Theta(r)/\log 2 - 1, \end{aligned}$$

where $\Theta(x) = \sum_p \log p$. Now [8, Theorem 9], states that for $x > 1$, $\Theta(x) < 1.01624x$. Applying this we find that for $r \leq 2n/5$,

$$r - 1 + \sum_{3 \leq p < r} \lfloor \log_2 p \rfloor < r + (1.017/\log 2)r < n$$

contradicting (33).

(b) This may be checked for values of $9 < n < 57$. If $n \geq 57$ we have $r(3, n) \geq 31$. Nagura [6] has shown that for $p' \geq 29$ we have $p' > 5p/6$. Applying this and part (a) of the lemma gives the result.

(c) Let $s(n)$ be the least prime satisfying $s(n) - 1 \geq n$. Clearly $s(n) \geq r(k, n)$ for all k so it is sufficient to show that $s(n) < 2n$, and this follows from Bertrand's Postulate.

We can now prove the main result for this section.

THEOREM 12. *If $\mathscr{A}$ is a collection of arithmetic progressions satisfying the conditions specified at the beginning of this section with $k \geq 3$ and $n \geq 12$ and p_0 being the least prime satisfying $p_0 > \sum_{p \geq p_0} c(p)$, then*

(a) $M(\mathscr{A}) < \dfrac{A(p_0)}{A(k)} V(W(p_0), p_0)2^n$, *and furthermore,*
(b) *if $r = r(k, n)$, then*

$$M(\mathscr{A}) < \frac{A(r)}{A(k)} V(W(r), r)2^n.$$

https://doi.org/10.1017/S1446788700000975 Published online by Cambridge University Press

PROOF. It follows from the fact that $\sum c(p) = n \geq 12$ and from inequality (26) that $p_0 \geq 7$. We set

$$X = \sum_{p \geq p_0} c(p) \tag{34}$$

which implies $X < p_0$. We then have

$$1 - \sum_{p \geq p_0} c(p)/p \geq 1 - X/p_0 > 0. \tag{35}$$

From (34) we have

$$2^{n-X} \prod_{p<p_0} 2^{-c(p)} = 1.$$

Using this and (34) in Corollary 6 (the use of which is justified by (35)) we obtain

$$\begin{aligned} M(\mathscr{A}) &< \frac{1+X}{1-X/p_0} 2^{n-X} \prod_{p<p_0} 2^{-c(p)} \frac{1+c(p)}{1-c(p)/p} \\ &= 2^n V(X, p_0) \prod_{p<p_0} V(c(p), p). \end{aligned}$$

We see by equation (25) that the product is not affected by factors corresponding to primes less than k. Applying Corollary 7 to each of the other factors we obtain

$$M(\mathscr{A}) < 2^n \frac{A(p_0)}{A(k)} V(X, p_0). \tag{36}$$

We now obtain some bounds on X in terms of p_0. The first comes from the definitions of X and p_0:

$$p_0 - 1 \geq X. \tag{37}$$

Next, let p_0' be the prime preceding p_0. By the definitions of X and p_0 and by inequality (26),

$$p_0' \leq \sum_{p \geq p_0'} c(p) \leq X + \lfloor \log_2 p_0' \rfloor.$$

This and inequality (37) give

$$W(p_0) \leq X \leq p_0 - 1. \tag{38}$$

Since X is an integer we have, by Theorem 11,

$$V(X, p_0) \leq \max\{V(W(p_0), p_0), V(p_0 - 1, p_0)\}. \tag{39}$$

https://doi.org/10.1017/S1446788700000975 Published online by Cambridge University Press

Using Lemma 1, Theorem 11, and the definition of $V(x, p)$ and the fact that $p_0 \geq 7$ we obtain

$$\frac{V(W(p_0), p_0)}{V(p_0 - 1, p_0)} \geq \frac{V(p_0 - 4, p_0)}{V(p_0 - 1, p_0)} = 2\frac{p_0 - 3}{p_0} > 1.$$

Thus the maximum in (39) is $V(W(p_0), p_0)$ and so by (36),

$$M(\mathscr{A}) < \frac{A(p_0)}{A(k)} V(W(p_0), p_0) 2^n. \tag{40}$$

This is part (a) of the theorem. We note that

$$X = n - \sum_{p < p_0} c(p) \geq n - \sum_{k \leq p < p_0} \lfloor \log_2 p \rfloor.$$

Combining this with inequality (37) we obtain

$$p_0 - 1 + \sum_{k \leq p < p_0} \lfloor \log_2 p \rfloor \geq n,$$

So that $p_0 \geq r(k, n)$. Using this inequality, Corollary 8 and (40), we obtain part (b) of the theorem.

For applications in the next section we use the following weaker but more convenient bound on $M(\mathscr{A})$.

COROLLARY 9. *If $\mathscr{A}$ is a collection of arithmetic progressions satisfying the conditions specified at the beginning of this section with $k \geq 3$ and $n \geq 12$ we have*

$$M(\mathscr{A}) \leq 16 \log 2 n^3 2^{2n/3} / A(k).$$

PROOF. With $r = r(k, n)$ and r' being the prime preceding r we have, using part (b) of the theorem and the definitions of V and W:

$$\begin{aligned} M(\mathscr{A}) &< \frac{A(r)(1 + r' - \lfloor \log_2 r' \rfloor)}{A(k)(r - r' + \lfloor \log_2 r' \rfloor)} r 2^{-r' + \lfloor \log_2 r' \rfloor + n} \\ &< \frac{A(r)(r')^2 r}{A(k) \log_2 r} 2^{-r' + n}. \end{aligned}$$

Using the estimates of Lemmas 2 and 3 we obtain the required inequality.

https://doi.org/10.1017/S1446788700000975 Published online by Cambridge University Press

4. Bounds on the cardinality of a minimal counter-example

In this section we obtain an upper bound on the cardinality of a minimal counter-example for arbitrary values of $k \geq 3$. This means that the conjecture could be verified for such values of k by checking a finite number of cases. The final section of the paper discusses this.

Let $\mathscr{A}$ be a minimal counterexample that does not cover 0; then by Corollary 3 each arithmetic progression in $\mathscr{A}$ lies in one of the following collections:

$$\mathscr{A}_L = \{S(d,a) \in \mathscr{A} : d \text{ is a product of primes } < k\},$$
$$\mathscr{A}_G = \{S(d,a) \in \mathscr{A} : d \text{ is a prime } \geq k\}.$$

Let $|\mathscr{A}_L| = n_L$ and $|\mathscr{A}_G| = n_G$, and let P be the least modulus such that there exists an arithmetic progression $S(P, A)$ satisfying $S(P, A) \cap (\cup \mathscr{A}_L) = \emptyset$. It follows from the Chinese Remainder Theorem that P divides $P(\mathscr{A}_L)$, that is, P is a product of primes less than k.

We now obtain two inequalities involving P. With g the function defined in the first section and using Theorem 1 we have

$$n_L \geq g(P), \tag{41}$$

and by Theorem 8 with $S(P, A)$ in the role of $S(d_0, a_0)$ if $P > 1$ and noting that $n_L = 0$ when $P = 1$, we have

$$n_L \leq \log_2 P. \tag{42}$$

THEOREM 13. *With P and $\mathscr{A}$ as defined in the previous paragraphs, $\pi(x)$ being the number of primes less than x and $\Theta(x) = \sum_p \log p$, where the sum is over all primes less than x, we have*

(a) $\log_2 P - g(P) \geq 0$,

(b) $\log_2 P - g(P) \leq \Theta(k)/\log 2 - \pi(k)$,

(c) $3\log_2 P - 2g(P) \leq \lceil \log_2 k \rceil + (3\log_2 3 - 4)\lceil \log_3 k \rceil + 3\Theta(k)/\log 2 - 2\pi(k) - 1$.

PROOF. Part (a) is an immediate consequence of inequalities (41) and (42). For parts (b) and (c) we suppose P has prime factorisation $P = \prod_{i=1}^{t} p_i^{\alpha_i}$. Then

$$\begin{aligned} \log_2 P - g(P) &= \sum_{i=1}^{t} (\alpha_i \log_2 p_i - (\alpha_i - 1)(p_i - 1) - 1) \\ &= \sum_{i=1}^{t} (\alpha_i (\log_2 p_i - p_i + 1) + p_i - 2). \end{aligned}$$

https://doi.org/10.1017/S1446788700000975 Published online by Cambridge University Press

The term in the inner brackets is at most 0 for any prime p_i so the expression is maximised when each $\alpha_i = 1$. Thus

$$\begin{aligned}\log_2 P - g(P) &\le \sum_{p<k} (\log_2 p_i - 1) \\ &= \Theta(k)/\log 2 - \pi(k),\end{aligned}$$

as required. This proves part (b). For part (c) we obtain

$$3\log_2 P - 2g(P) = \sum_{i=1}^{t} (\alpha_i(3\log_2 p_i - 2p_i + 2) + 2p_i - 4).$$

This time the term in the inner pair of brackets is negative for $p_i > 3$. If p_i equals 2 or 3 we apply Corollary 5. This leads to

$$\begin{aligned}&3\log_2 P - 2g(P) \\ &\quad\le \lceil \log_2 k\rceil(3\log_2 2 - 2) + (1 + \lceil\log_3 k\rceil)(3\log_2 3 - 4) + 2 + \sum_{3<p<k}(3\log_2 p - 2) \\ &\quad\le \lceil\log_2 k\rceil + (3\log_2 3 - 4)\lceil\log_3 k\rceil + 3\Theta(k)/\log 2 - 2\pi(k) - 1,\end{aligned}$$

as required.

We can now prove our main theorem.

THEOREM 14. *If $\mathscr{A}$ is a minimal counterexample for some $k \ge 3$, then n is less than*

$$3(\Theta(k)/\log 2 + k) - 2\pi(k) + 36\log_2 k + \lceil\log_2 k\rceil + (3\log_2 3 - 4)\lceil\log_3 k\rceil - 4.$$

PROOF. We assume, without loss of generality, that $\mathscr{A}$ does not cover 0. Since $\bigcup \mathscr{A}_L \cap S(P, A) = \emptyset$ we must have $\bigcup \mathscr{A}_G \supseteq S(P, A) \cap [1, k2^{n-k+1}]$.

Reducing $\mathscr{A}_G$ via $S(P, A)$ we obtain a collection $\mathscr{A}_G*$ which satisfies conditions (24) to (26) and such that $\cup\mathscr{A}_G*$ contains $\lfloor k2^{n-k+1}/P\rfloor$ consecutive integers. By adjusting the residues of the arithmetic progressions in $\mathscr{A}_G*$ we can form another collection $\mathscr{A}_G**$, say, for which $M(\bigcup \mathscr{A}_G **) \ge \lfloor k2^{n-k+1}/P\rfloor$. We use this to obtain an upper bound for n_G in terms of k and P. We first assume that $n_G \ge 12$. From Corollary 9 we then have

$$16\log 2n_G^3 2^{2n_G/3}/A(k) > k2^{n-k+1}/P - 1.$$

Noting that

$$n = n_G + n_L, \tag{43}$$

https://doi.org/10.1017/S1446788700000975 Published online by Cambridge University Press

and rearranging we obtain

$$(44)\qquad 16\log 2n_G^3 2^{-n_G/3} > kA(k)2^{-k+1+n_L-\log_2 P} - A(k)2^{-n_G}.$$

We claim this implies

$$(45)\qquad n_G < 3(k-1-n_L+\log_2 P+12\log_2 k).$$

To show this suppose that this inequality does not hold. Then, for $k \geq 3$ and using inequality (42) we see that $n_G > 12$. For such n_G the left-hand side of (44) is decreasing, so it is sufficient to consider the value of the left-hand side of (44) when

$$n_G = 3(k-1-n_L+\log_2 P+12\log_2 k).$$

We find, using inequality (41), part (b) of Theorem 13 and this value of n_G that,

$$\begin{aligned}&16\log 2n_G^3 2^{-n_G/3}\\ &\qquad \leq 432\log 2(k-1+\Theta(k)/\log 2-\pi(k)+12\log_2 k)^3 k^{-13} 2^{-k+1+n_L-\log_2 P}.\end{aligned}$$

Now

$$432\log 2(k-1+\Theta(k)/\log 2-\pi(k)+12\log_2 k)^3 k^{-13}$$

is decreasing with k, and when $k=3$ it equals $0.6574\ldots$, and so

$$16\log 2n_G^3 2^{-n_G/3} < k2^{-k+1+n_L-\log_2 P}$$

and is certainly less than the right-hand side of (44). This establishes inequality (45) in the case $n_G \geq 12$.

If $n_G < 12$ it is easy to see that inequality (42) still holds using our assumption that $k \geq 3$ and inequality (42). We now obtain our bound on n. Using (43), (41) and (45) we have

$$\begin{aligned}n &< 3(k-1-n_L+\log_2 P+12\log_2 k)+n_L\\ &\leq 3k-3+36\log_2 k+3\log_2 P-2g(P).\end{aligned}$$

Applying part (c) of Theorem 13 gives the inequality of the theorem.

5. Discussion

We have shown that if a counterexample to the conjecture exists for a given k then one exists for that k and n bounded by the expression in Theorem 14. For such an n

https://doi.org/10.1017/S1446788700000975 Published online by Cambridge University Press

there are a finite number of ways the interval $\{1, \ldots, k2^{n-k+1}\}$ can be partitioned into n sets, so we could examine each of these to see whether any corresponds to a set of arithmetic progressions with common differences greater than or equal to k. If none did the conjecture would hold for this value of k.

Although possible in principle, the time required for such an undertaking would be prohibitive, even for low k. A more practical method is to run through the values of n allowed by Theorem 14, and for each of these consider the cases $n_g = 0, \ldots, n$. We can get a bound on the maximum value the function $M(\mathscr{A})$ can take for these values of k and n_G using part (b) of Theorem 12. Note that this is much stronger than Corollary 9 since the value of the bound can be calculated exactly rather than relying on the weak bounds of Lemmas 2 and 3. As in the proof of Theorem 12 we have $M(\mathscr{A}) \geq k2^{n-k+1}/P$ which becomes

$$\log_2 P \geq \log_2(k2^{n-k+1}/M(\mathscr{A})),$$

which gives an explicit lower bound on $\log_2 P$. Using part (b) of Theorem 13 and (41) we get a lower bound on n_L. For most values of n and n_G this bound will be incompatible with $n_L + n_G = n$. This process will get rid of most $\{n_L, n_G\}$ pairs. Those remaining must be considered separately: in each the set of allowable arithmetic progressions is restricted by the various conditions obtained in Section 2. In estimating $M(\mathscr{A})$ primes which are greater than $M(\mathscr{A})$ can only cover one integer in $[1, M(\mathscr{A})]$ so such primes are all equivalent. The process has been performed successfully for the $k = 3$ case [10].

Acknowledgements

This paper is based on work done for my doctoral thesis at The University of Adelaide and written, sometime later, while visiting Illinois State University. I thank the faculty at both institutions for their help and friendship, and Charles Vanden Eynden for his useful advice. I most particularly thank my doctoral supervisor, Jane Pitman.

References

[1] R. B. Crittenden and C. L. Vanden Eynden, 'Any n arithmetic progressions covering the first 2^n integers cover all the integers', *Proc. Amer. Math. Soc.* **24** (1970), 475–481.

[2] ———, 'The union of arithmetic progressions not less than k', *Amer. Math. Monthly* **79** (1972), 630.

[3] P. Erdös, 'Remarks on number theory IV : extremal problems in number theory I', *Mat. Lapok* **13** (1962), 241–243 (Hungarian, English summary).

https://doi.org/10.1017/S1446788700000975 Published online by Cambridge University Press

[4] R. K. Guy, *Unsolved problems in number theory* (Springer, Berlin, 1980), pp. 140–141.

[5] W. J. Leveque, *Fundamentals of number theory* (Addison-Wesley, Reading, 1977).

[6] J. Nagura, 'On the interval containing at least one prime number', *Proc. Japan Acad.* **28** (1952), 177–181.

[7] S. Porubsky, 'Results and problems on covering systems of congruences', *Czechoslovak Math. J.* **24** (1974), 598–606.

[8] G. Barkley Rosser and L. Schoenfeld, 'Approximate formulas for some functions of prime numbers', *Illinois J. Math.* **6** (1962), 64–94.

[9] J. Selfridge, *Research announcement*, Amer. Math. Soc. Annual Meeting (New Orleans, 1969).

[10] R. J. Simpson, *Covering the integers with arithmetic progressions* (Ph. D. Thesis, University of Adelaide, 1982).

[11] ———, 'Regular coverings the integers by arithmetic progressions', *Acta Arithmetica* **45** (1985), 145–152.

[12] S. K. Stein, 'Unions of arithmetic sequences', *Math. Ann.* **134** (1958), 289–294.

School of Mathematics
Curtin University of Technology
Perth, WA 6001
Australia
e-mail: simpson@cs.curtin.edu.au

https://doi.org/10.1017/S1446788700000975 Published online by Cambridge University Press