COVERING THE INTEGERS WITH ARITHMETIC PROGRESSIONS

by

R.J. Simpson

A Thesis submitted for the
Degree of Doctor of Philosophy
at the University of Adelaide,
Department of Pure Mathematics.

November, 1984.

awarded 1-4-85

TABLE OF CONTENTS

SUMMARY

A *regular covering system* is a collection of arithmetic progressions such that every integer belongs to at least one arithmetic progression in the collection, and no proper subcollection has this property.

An *exact covering system* is a regular covering system with the property that every integer belongs to exactly one of the arithmetic progressions.

The thesis contains three principal results.

1. Let P be the lowest common multiple of the common differences of the arithmetic progressions in a regular covering system and suppose P has prime factorisation

$$P = \prod_{i=1}^{t} p_i^{\alpha_i} .$$

Then the number of arithmetic progressions in the collection is at least

$$\sum_{i=1}^{t} \alpha_i (p_i - 1) + 1.$$

A similar result has been proved by Korec [4] applied to exact covering systems. In both cases the results are the best possible.

2. An exact covering system in which each common difference occurs at most M times is called an ECS(M).

I prove the following result. If $p_1 < p_2 \ldots < p_t$ are the distinct prime divisors of the lowest common multiple of the common differences of the arithmetic progressions in an ECS(M) then

$$M \prod_{i=1}^{t-1} p_i/(p_i-1) \geqslant p_t$$

Burshtein [1] showed that a similar inequality applied in the case of a special type of exact covering system called a naturally exact covering system. Our result has several consequences. For instance it follows that in any ECS(M) we have $p_1 \leqslant M$ and that there exists a number $B(M)$ such that any ECS(M) contains an arithmetic progression with common difference less than $B(M)$.

3. The last part of this thesis concerns the following conjecture due to R.B. Crittenden and C.L. Vanden Eynden [3].

Let S be the union of n arithmetic progressions, each with common difference not less than k where $k \leqslant n$. It is conjectured that if S contains the closed interval $[1, k\,2^{n-k+1}]$ then S contains all integers.

Crittenden and Vanden Eynden [2] proved the conjecture in the (equivalent cases corresponding to $k = 1$ and $k = 2$. I prove the conjecture in the case $k = 3$ and show that if a counterexample exists for a given k then a counterexample exists for that k with the following properties:

(a) Each common difference in the counterexample is either a prime $\geqslant k$ or a product of primes $< k$.

(b) If p is a prime, $p \geqslant k$, then the number of arithmetic progressions with common difference p is less than $\log p/\log 2$.

(c) The cardinality of the collection is less than an explicit function of k, that function being asymptotically equal to $3k(1 + 1/\log 2)$ as $k \to \infty$.

References

[1] N. Burshtein, "On natural exactly covering systems of congruences having moduli occurring at most N times", Discrete Math. 14(1976), 205-214.

[2] 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.

[3] R.B. Crittenden and C.L. Vanden Eynden, "The union of arithmetic progressions with differences not less than k", Am. Math. Monthly 79(1972), 630.

[4] I. Korec, "On a generalisation of Mycielski's and Znam's conjectures about coset decomposition of Abelian Groups", Fund. Math. 85(1974), 41-48.

SIGNED STATEMENT

This thesis contains no material which has been submitted for the award of any other degree or diploma.

To the best of my knowledge this thesis contains no material previously published by another person, except where due reference is made in the text of the thesis.

I consent to this thesis being made available for photocopying and loan.

James Simpson

PUBLICATIONS ARISING FROM THIS THESIS

"Regular coverings of the integers by arithmetic progressions", to appear, Acta Arithmetica 45 (1985), 63-70.

"Exact coverings of the integers by arithmetic progressions", submitted to the Journal of Discrete Mathematics.

ACKNOWLEDGEMENTS

My principal thanks are due to my supervisor, Jane Pitman, who has been of immense assistance in all aspects of this work. All the major proofs in this thesis are the results of corrections and simplifications suggested by her. My wife Judy has encouraged me in times of gloom and depression, been patient in times of bad temper and even endured my overweening conceit when things have gone well. For this I am very grateful. I also thank Mrs. Dawn Darwent for her excellent and meticulous typing.

Finally I wish specifically to exclude from these acknowledgements my son Tom, whose riotous behaviour and incontinent disposition did much to hamper the last eighteen months of the work.

Jamie Simpson

CHAPTER 1

INTRODUCTION

If S is a set of integers and A is a collection of arithmetic progressions with the property that every integer in S belongs to at least one of the arithmetic progressions in A we say that A *covers* S. If the set S is the set of integers we say that A is a *covering system*.

The idea of covering systems was introduced by Erdös [7] in 1950. He used such a system to answer a question posed by Romanoff: are there infinitely many odd integers not of the form $2^k + p$ where p is a prime? The answer was yes.

A covering system may be regarded as a collection of congruence classes $a_i \pmod{m_i}$, $1 \leqslant i \leqslant k$ with $m_1 \leqslant m_2 \leqslant \ldots \leqslant m_k$, which has the property that every integer n satisfies

$$n \equiv a_i \pmod{m_i}$$

for at least one value of i. Erdös used covering systems in which the m_i's are distinct. We will call such systems *incongruent covering systems*, a name coined by Porubsky [19], (Erdös simply called them covering systems).

There are a number of unsolved problems connected with incongruent covering systems (see, for instance, Guy [11]), the best known being:

I Are there incongruent covering systems with m_1 arbitrarily large?

II Are there incongruent covering systems with all the m_i's odd?

These questions have attracted considerable interest but little in the way of general results. We will make a few remarks about question II in Chapter 4, but for most of this thesis we will be concerned with problems about other types of covering systems.

There are several different types of covering systems and a large literature associated with them. In his useful monograph on the subject, Porubsky [19] cites over 100 articles. Some authors have used complex analysis in investigating covering systems, though most of the literature uses elementary combinatorial ideas. In this thesis we rely entirely on combinatorics.

We will consider three questions about types of covering systems. The questions themselves are not closely related, but the techniques used in attacking them are similar. In particular, in definition 2.7 we introduce a tool which we call *reducing* a collection of arithmetic progressions. This will be used in many of the proofs. It involves taking a collection of arithmetic progressions which intersect a given arithmetic progression and

transforming it into a new collection. The way in which the new collection is related to the integers is implied by the way the original collection was related to the given arithmetic progression. For instance, if the original collection covers the given arithmetic progression then the new collection will cover the integers.

Before describing the questions in which we are interested we introduce some notational devices.

Notation 1.1

The terms *congruence class* and *arithmetic progression* are used interchangeably in the literature and we will retain this admirable flexibility. We will however always use the term *modulus* rather than common difference of an arithmetic progression. Henceforth we will write AP for arithmetic progression.

Collections of AP's will be denoted by script capitals: $\mathcal{A}$, $\mathcal{B}$, $\mathcal{C}$ etc. For a given collection $\mathcal{A}$ we write $P(\mathcal{A})$ for the lowest common multiple of the moduli of the AP's occurring in $\mathcal{A}$, $Z(\mathcal{A})$ for the union of the AP's in $\mathcal{A}$ and $|\mathcal{A}|$ for the number of AP's in $\mathcal{A}$. We write $\langle a,d \rangle$ for the AP consisting of integers congruent to a modulo d.

We say $\mathcal{A}$ is a *regular covering system* if $Z(\mathcal{A}) = \mathbb{Z}$, where $\mathbb{Z}$ is the set of integers, and if no subcollection of $\mathcal{A}$ has this property. The name regular covering comes from Znam, *irredundant covering* is also used in the literature with the same meaning.

We say A is an *exact covering system* if A is a regular covering and no integer belongs to more than one of the AP's in A. *Disjoint covering* is an alternative name in the literature.

The following special functions will be used in Chapters 3 and 7. If a positive integer n has prime factorisation

$$n = \prod_{i=1}^{n} p_i^{\alpha_i}$$

then

$$f(n) = \sum_{i=1}^{t} \alpha_i (p_i - 1)$$

$$g(n) = \sum_{i=1}^{t} \left((\alpha_i - 1)(p_i - 1) + 1 \right)$$

Our first main result will be the following.

Corollary 3.5 If A is a regular covering then

$$|A| \geq f(P(A)) + 1.$$

This result, which was conjectured by Znam [26] in 1975, was preceded by several weaker conjectures and their proofs dating back to a conjecture made by Mycielski and Sierpinski [16] in 1966. A detailed background is given in Chapter 3, together with the proof and some extensions.

In Chapter 3 we will also prove

Theorem 3.9. If A is a collection of AP's that does not cover the integers and P is the minimum modulus for which

there exists an AP $\langle a,P\rangle$ such that

$$Z(A) \cap \langle a,P\rangle = \phi,$$

then

$$|A| \geq g(P).$$

The second main result is an extension of work by Burshtein [2], [3].

Theorem 4.12 If A is an exact covering system in which each modulus appears at most M times and $p_1 < p_2 < \ldots < p_t$ are the distinct prime divisors of P(A) then

$$M \prod_{i=1}^{t-1} \frac{p_i}{p_i - 1} \geq p_t .$$

The theorem has several interesting consequences. These appear in Chapter 4.

The last three chapters deal with the following conjecture made by Crittenden and Vanden Eynden [5].

Conjecture 5.1 If A is a collection of AP's, each with modulus at least k, and

$$Z(A) \supseteq [1, k2^{n-k+1}]$$

then

$$Z(A) = \mathbb{Z}$$

The cases k=1 and k=2 (which are equivalent since $k2^{n-k+1}$ is the same for k=1 and k=2) were proven by Crittenden and Vanden Eynden [4] in 1970. In Chapter 7 we prove the conjecture in the case k=3. We also obtain,

in Chapters 5 and 7 some strong necessary conditions for the conjecture to be false. The most important of these is that if the conjecture fails for some k then it fails for that k and a value of n less than an explicit function of k, this function being asymptotically equal to

$$3(1 + 1/\log 2)k$$

as $k \to \infty$.

This means that the conjecture could be proven for arbitrary k by checking that it holds for that k and all low values of n. This checking is carried out in Chapter 7 for the case $k=3$. In Chapter 7 we will also make another conjecture akin to conjecture 5.1 and show that it can be analysed in a similar way.

Chapter 2 of the thesis contains a number of technical lemmas used in later chapters. Most of these have little intrinsic interest and the reader may prefer to move straight into Chapter 3 and return to Chapter 2 only to inspect its parts as they are cited.

Notation 1.2 Letters in ordinary typeface, upper or lower case, will represent integers unless otherwise stated. Script capitals will represent sets or collections of AP's.

$\|A\|$	the cardinality of the set or collection A.
$\langle a,d \rangle$	the AP $\{n : n \equiv a \pmod d\}$.
f,g	the functions defined in notation 1.1.
(m,n)	the highest common factor of the integers m and n.

$[m,n]$	the block of consecutive integers $m, m+1, \ldots, n$.
$\ell cm\{m,n\}$	the least common multiple of the integers m and n.
$m \mid n$	m divides n.
$m \nmid n$	m does not divide n.
$[x]$	the greatest integer not greater than the real number x.
$\lceil x \rceil$	the least integer not less than the real number x.
$\log_k x$	logarithm to the base k of x.
$P(A)$	the lowest common multiple of the moduli of the AP's in the collection A.
p,q	prime numbers, often used with subscripts.
$p^\alpha \| n$	p^α divides n, but $p^{\alpha+1}$ does not divide n.
$Z(A)$	the union of the AP's in the collection A.
$\mathbb{Z}$	the integers
$\mathbb{Z}_n$	the ring of integers $0,1, \ldots, n-1$ (modulo n).
γ	Euler's constant; 0.57721566...
$\theta(x)$	$\sum_{p \leq x} \log p$
$\mu(n)$	the Möbius function
$\nu(n)$	the number of distinct prime divisors of n.
$\pi(x)$	the number of primes less than or equal to x.
$\prod$	product, empty products equal 1.

$\sum$ sum, empty sums equal 0.

ϕ empty set.

Theorems, lemmas, corollaries et cetera will be labelled m.n where m is the chapter in which the theorem occurs and n is an integer which begins at 1 in each chapter and is incremented by 1 with each theorem, lemma et cetera. Thus lemma 2.3 immediately precedes theorem 2.4.

Displays are labelled (m) where m is an integer which begins at (1) in each chapter and is incremented by 1 for each display.

CHAPTER 2

TECHNICAL RESULTS ABOUT ARITHMETIC PROGRESSIONS

In this chapter we prove some basic results about AP's and collections of AP's. They will be used to prove the more involved results of later chapters. Not all are original to this work but proofs of all of them will be given for the sake of completeness.

The first three deal with properties of intersecting AP's and are fairly easy consequences of the Chinese Remainder Theorem, indeed part (a) of theorem 2.1 is just a restatement of that theorem. Here and elsewhere we say two or more AP's intersect if their common intersection is non empty. We use notation 1.2.

Theorem 2.1

(a) $\langle A,D\rangle$ and $\langle a,d\rangle$ intersect if and only if

$$a \equiv A \pmod{(d,D)}.$$

(b) If $\langle A,D\rangle$ and $\langle a,d\rangle$ do intersect then

$$\langle A,D\rangle \cap \langle a,d\rangle = \langle a^*, \ell cm\{D,d\}\rangle$$

for some a^*.

(c) If d divides D then either $\langle A,D\rangle \subseteq \langle a,d\rangle$ or $\langle A,D\rangle$ and $\langle a,d\rangle$ are disjoint.

(d) $\langle A,D\rangle \subseteq \langle a,d\rangle$ if and only if d divides D and

$$a \equiv A \pmod{d}.$$

(e) If $\langle a,d\rangle$ intersects both $\langle A_1,D_1\rangle$ and $\langle A_2,D_2\rangle$ then

$$A_1 \equiv A_2 \ (\mathrm{mod}(d,D_1,D_2)).$$

Proof:

(a) $\langle A,D\rangle$ and $\langle a,d\rangle$ intersect if and only if there exists an integer n such that

$$n \equiv a \ (\mathrm{mod}\ d)$$
$$n \equiv A \ (\mathrm{mod}\ D). \qquad (1)$$

By the Chinese Remainder theorem this is possible if and only if

$$a \equiv A \ (\mathrm{mod}(d,D)).$$

(b) Again by the Chinese Remainder theorem (Hua, [12]), if the congruences (1) are satisfied then they are satisfied by exactly one residue class modulo $\ell\mathrm{cm}\{d,D\}$. If this residue class is a^* $(\mathrm{mod}\ \ell\mathrm{cm}\{d,D\})$ then we see that the intersection of the AP's is

$$\langle a^*, \ell\mathrm{cm}\{d,D\}\rangle.$$

(c) Suppose that d divides D and $\langle a,d\rangle$ intersects $\langle A,D\rangle$. Then it follows from (b) that the intersection of these two AP's is an AP of the form $\langle a^*,D\rangle$ and so must coincide with $\langle A,D\rangle$. Hence $\langle A,D\rangle$ is a subset of $\langle a,d\rangle$.

(d) If $\langle A,D\rangle$ is a subset of $\langle a,d\rangle$ then the intersection of these two AP's is $\langle A,D\rangle$ and hence, by (b), we have $D = \ell\mathrm{cm}\{d,D\}$ and so d divides D.

By (a)

$$a \equiv A \ (\mathrm{mod}(d,D))$$

and $(d,D) = d$ since d divides D.

In the other direction d divides D and

$$a \equiv A \ (\mathrm{mod}\ d)$$

imply

$$a \equiv A \ (\mathrm{mod}(d,D)).$$

Therefore the AP's intersect by part (a) and then by part (c)

$$\langle A,D\rangle \subseteq \langle a,d\rangle.$$

(e) By (a) we have

$$a \equiv A_1 \ (\mathrm{mod}(d,D_1))$$

and

$$a \equiv A_2 \ (\mathrm{mod}(d,D_2))$$

which imply the result. □

Most of the results here appear in texts on elementary number theory, see e.g. Shockley [22] theorem 6 of Chapter 3. The next result appears in Leveque [15] theorem 3.16, though proved there in a different way.

Theorem 2.2 Let $A = \{\langle a_i,d_i\rangle : i = 1, \ldots, t\}$ be a collection of AP's. (a) The collection has a nonempty intersection if and only if each pair of AP's in A has. (b) The intersection is then an AP with modulus $\mathrm{lcm}\{d_1,d_2, \ldots, d_t\}$.

Proof:

(a) In one direction the result is immediate. In the other direction we use induction on t. The result clearly holds when $t = 2$. We assume it holds for $t = t_0$ and will show it holds for $t = t_0 + 1$.

By part (b) of theorem 2.1 we have

$$\langle a_1, d_1 \rangle \cap \langle a_2, d_2 \rangle = \langle a^*, \ell cm\{d_1, d_2\} \rangle$$

where

$$a^* \equiv a_1 \pmod{d_1}$$

$$a^* \equiv a_2 \pmod{d_2}$$

Now for $i = 3, \ldots, t_0 + 1$ we have

$$a_i \equiv a_1 \left(\mathrm{mod}(d_1, d_i)\right)$$

$$\equiv a^* \left(\mathrm{mod}(d_1, d_i)\right)$$

and similarly

$$a_i \equiv a^* \left(\mathrm{mod}(d_2, d_i)\right).$$

These imply

$$a_i \equiv a^* \left(\mathrm{mod}\ \ell cm\{(d_1, d_i), (d_2, d_i)\}\right),$$

that is

$$a_i \equiv a^* \left(\mathrm{mod}(d_i, \ell cm\{d_1, d_2\})\right).$$

It follows, by theorem 2.1 part (a), that the AP's $\langle a^*, \ell cm\{d_1, d_2\} \rangle$ and $\langle a_i, d_i \rangle$ have a non empty intersection so that we have the t_0 AP's

$$\langle a^*, \ell cm\{d_1, d_2\} \rangle, \ \langle a_3, d_3 \rangle, \ \ldots \ \langle a_{t_0+1}, d_{t_0+1} \rangle$$

intersecting in pairs and so, by the induction hypothesis, the collection has a non empty intersection.

(b) This part is also proved by induction on t. By theorem 2.1, part (b) $\langle a_1,d_1\rangle \cap \langle a_2,d_2\rangle$ has modulus $\ell cm\{d_1,d_2\}$. Then

$$\{\langle a_1,d_1\rangle \cap \langle a_2,d_2\rangle\} \cap \langle a_3,d_3\rangle$$

has modulus $\ell cm\{\ell cm\{d_1,d_2\},d_3\} = \ell cm\{d_1,d_2,d_3\}$ and so on so that

$$\bigcap_{i=1}^{t} \langle a_i,d_i\rangle$$

has modulus $= \ell cm\{d_1,d_2, \ldots, d_t\}$. □

Lemma 2.2 is used to prove the next theorem.

Lemma 2.3 Let $A = \{\langle a_i,d_i\rangle : i = 1,\ldots,t\}$ be a collection of AP's and P a common multiple of $d_1,d_2,\ldots,d_t$. Then the number of residue classes modulo P that are covered by A is at least

$$P\left\{\sum_{i=1}^{t} \frac{1}{d_i} - \sum_{1\leqslant i<j\leqslant t} \frac{1}{[d_i,d_j]} + \sum_{1\leqslant i<j<k\leqslant t} \frac{1}{[d_i,d_j,d_k]} - \ldots\right\}, \qquad (2)$$

where square brackets denote lowest common multiple.

This bound is best possible and therefore positive.

Proof: We write $N(i_1,i_2,\ldots,i_s)$ for the number of residue classes modulo P covered by the intersection of $\langle a_i,d_i\rangle,\ldots,\langle a_i d_i\rangle$. By inclusion-exclusion the number of residue classes covered by A is

$$\sum_{1\leqslant i\leqslant t} N(i) - \sum_{1\leqslant i<j\leqslant t} N(i,j) + \ldots \qquad (3)$$

We note that if d divides P then the number of residue classes modulo P covered by an AP with modulus d is

$$\frac{P}{d} \tag{4}$$

Now for each pair i,j satisfying

$$1 \leqslant i < j \leqslant t$$

we set

$$\varepsilon(i,j) = \begin{cases} 1 & \text{if } \langle a_i,d_i\rangle \cap \langle a_j,d_j\rangle \neq \phi, \\ 0 & \text{otherwise.} \end{cases}$$

By lemma 2.2 we see that

$$\langle a_{i_1},d_{i_1}\rangle \cap \ldots \cap \langle a_{i_s},d_{i_s}\rangle \neq \phi$$

if and only if

$$\prod\prod \varepsilon(i_j,i_k) = 1,$$

where the product runs over all pairs of distinct elements of $\{i_1,\ldots,i_s\}$. Using this observation and (3) above we see that the number of residue classes modulo P covered by A equals

$$\sum \frac{P}{d_i} - \sum \frac{P\varepsilon(i_1,i_2)}{[d_{i_1},d_{i_2}]} + \sum \frac{P \prod\prod \varepsilon(i_j,i_k)}{[d_{i_1},d_{i_2},d_{i_3}]} - \ldots \tag{5}$$

where the product is over all pairs i_j,i_k from i_1, i_2, i_3 and each ε equals 0 or 1. We claim that this expression is minimised when each ε equals 1.

To show this we consider the sum of all those terms in (5) which contain a factor $\varepsilon(1,2)$. This is

$$- P\,\varepsilon(1,2)\left\{ \frac{1}{[d_1,d_2]} - \sum_{2<i\leqslant t} \frac{\varepsilon(1,i)\varepsilon(2,i)}{[d_1,d_2,d_i]} + \ldots \right\}$$

$$= -\{N(1,2) - \Sigma N(1,2,i) + \ldots\}. \qquad (6)$$

The expression in the brackets is the number of residue classes modulo P which are covered by the intersection of $\langle a_1,d_1\rangle$ and $\langle a_2,d_2\rangle$ and are not covered by any other AP in A. This is clearly non-negative and so the expression in (6) in non-positive. Thus changing the value of $\varepsilon(1,2)$ from 0 to 1 can only decrease the value of expression (5). The same argument applies to any $\varepsilon(i,j)$ so (5) attains its minimum as a function of the $\varepsilon(i,j)$'s when each $\varepsilon(i,j)$ is set equal to 1. In this case (5) reduces to (2) as required.

Finally we note that it is possible to have each pair of AP's in A intersecting, for instance when all the a_i's are equal. In this case (5) coincides with (2) and so (2) is best possible. □

In this work we will be concerned with the conditions under which a collection of AP's covers the integers. A technique that we will use extensively is to concentrate on how a collection covers a single AP (or part of it) and to deduce properties of the whole collection. The remaining results of this chapter are tools that will be used in employing this technique.

In the next theorem we use the notation $Z(A)$ and $P(A)$ which is explained in notation 1.1.

Theorem 2.4 If A is a collection of AP's such that

$$Z(A) \supseteq \langle A,D \rangle$$

$$Z(A) \neq \mathbb{Z}$$

for some AP $\langle A,D \rangle$, then

(a) A contains an AP $\langle a,d \rangle$ with $(d,D) > 1$,

(b) this AP intersects $\langle A,D \rangle$.

Proof:

(a) We prove this part by contradiction. If it were not true then we would have

$$(D,P(A)) = 1.$$

By assumption there is some integer x_0 which does not belong to any AP in A. Clearly this will also be so for any integer congruent to x_0 modulo $P(A)$. Now choose, as we may by the Chinese Remainder Theorem, an integer x satisfying

$$x \equiv x_0 \pmod{P(A)}$$

$$x \equiv A \pmod{D}.$$

Then x does not belong to $Z(A)$ but does belong to $\langle A,D \rangle$, contradicting the assumption that A covers $\langle A,D \rangle$.

(b) If we removed from A all those AP's which do not intersect A, forming a new collection A^*, say, then the premises of the theorem would still hold

with A^* replacing A. Therefore by part (a), A^* contains an AP $\langle a,d\rangle$ with $(d,D) > 1$ which intersects $\langle A,D\rangle$. This AP belongs to A and the theorem follows. □

In applications we will use the following corollaries to this theorem.

Corollary 2.5 If A is a collection of AP's such that

$$Z(A) \supseteq \langle A,p\rangle$$
$$Z(A) \neq \mathbb{Z}$$

for some AP $\langle A,p\rangle$ where p is a prime, then A contains an AP $\langle a,d\rangle$ such that

(a) $p \mid d$

(b) $\langle a,d\rangle \subseteq \langle A,p\rangle$

Proof: Part (a) follows immediately from (a) of theorem 2.4 on setting $D = p$. By (b) of that theorem $\langle a,d\rangle$ intersects $\langle A,p\rangle$ so that (b) of the corollary follows from (c) of theorem 2.1. □

A result similar to the next corollary was proved by Billick and Edgar [1] using a rather esoteric method which involved representing an AP as a vector whose entries were the residue classes to which the members of the AP belonged modulo the prime divisors of the modulus.

In theorem 3.1 of the next chapter we will extend corollary 2.6 considerably, and use the extension to prove the main result of that chapter. The present simpler result is more convenient for applications in Chapter 5.

Corollary 2.6 If $A = \{\langle a_i, d_i\rangle : i = 1,\ldots,t\}$ is a regular covering system (see notation 1.1), and p is a prime dividing $P(A)$ then the set

$$\{a_i : p \mid d_i\}$$

contains a complete residue system modulo p.

Proof: Since p divides $P(A)$, A contains some AP, $\langle a_j, d_j\rangle$ say, in which p divides d_j. We must show that for any A satisfying

$$A \not\equiv a_j \pmod{p}$$

there exists an AP $\langle a_k, d_k\rangle$ in A with p dividing d_k and

$$a_k \equiv A \pmod{p}.$$

Fix such an A and remove $\langle a_j, d_j\rangle$ from A to form a new collection A^*. Since $\langle a_j, d_j\rangle$ does not intersect $\langle A, p\rangle$ (by (a) of theorem 2.1) we have

$$Z(A^*) \supseteq \langle A, p\rangle$$
$$Z(A^*) \neq \mathbb{Z}$$

By corollary 2.7 A^* contains an AP $\langle a_k, d_k\rangle$ with p dividing d_k and $\langle a_k, d_k\rangle$ included in $\langle A, p\rangle$. By (d) of theorem 2.1 this implies

$$a_k \equiv A \pmod{p}$$

as required. □

We will now introduce a method which we will call *reducing* a collection of AP's. To get an idea of the method

consider the pair of AP's $\langle 0,10\rangle$ and $\langle 5,10\rangle$. These cover the AP $\langle 0,5\rangle$, since $\langle 0,10\rangle$ consists of the even elements of $\langle 0,5\rangle$ and $\langle 5,10\rangle$ of the odd elements. In some sense $\langle 0,10\rangle$ and $\langle 5,10\rangle$ are analogous to $\langle 0,2\rangle$ and $\langle 1,2\rangle$ which are, in some sense, simpler than the original pair of AP's. We will now formalise and generalise this idea. We define a method for transforming a collection of AP's which intersect a given AP, say $\langle A,D\rangle$, into another collection which covers a subset of the integers which is analogous to the subset of $\langle A,D\rangle$ covered by the original collection.

Definition 2.7 Suppose we have a collection of AP's

$$A = \{\langle a_i,d_i\rangle : i = 1,\ldots,s,\ldots,t\}$$

where $s \leqslant t$ and an AP $\langle A,D\rangle$, and suppose that $\langle A,D\rangle$ intersects $\langle a_i,d_i\rangle$ for $i = 1,\ldots,s$, and not for i greater than s.

We set

$$\delta_i = (D,d_i)$$

for $i = 1,\ldots,s$. Now form another collection

$$A^* = \{\langle a_i^*,d_i^*\rangle : i = 1,\ldots,s\}$$

where

$$d_i^* = d_i/\delta_i \tag{7}$$

and

$$a_i^* D/\delta_i \equiv (a_i - A)/\delta_i \pmod{d_i^*} \tag{8}$$

We call A^* the *reduction of* A *via* $\langle A,D\rangle$ and $\langle a_i^*,d_i^*\rangle$ the *reduction of* $\langle a_i,d_i\rangle$ *via* $\langle A,D\rangle$.

Remark 2.8 Note that δ_i divides $a_i - A$ by (a) of theorem 2.1, and that D/δ_i and d_i^* are relatively prime so a_i^* is uniquely defined modulo d_i^*.

Remark 2.9 If D divides d_i, (8) simplifies to

$$a_i^* \equiv \frac{a_i - A}{D} \pmod{d_i^*}.$$

The next theorem and its corollary give the useful properties of the reduction technique. We will use it extensively in the following chapters.

Theorem 2.10 Suppose $\langle a^*,d^* \rangle$ is the reduction of $\langle a,d \rangle$ via $\langle A,D \rangle$. Then if n is any integer

$$A + nD \in \langle a,d \rangle$$

if and only if

$$n \in \langle a^*,d^* \rangle.$$

Proof: We set

$$\delta = (d,D).$$

By (a) of theorem 2.1 and the definition of reduction we have

$$A \equiv a \pmod{\delta}$$

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

Now,

$$A + nD \in \langle a,d \rangle$$

$$\Leftrightarrow \quad nD \equiv a - A \pmod{d}$$

$$\Leftrightarrow \quad nD/\delta \equiv a^*D/\delta \pmod{d/\delta}$$

$\Leftrightarrow \quad n \equiv a^* \pmod{d/\delta}$

$\Leftrightarrow \quad n \in \langle a^*, d^* \rangle$.

□

Definition 2.11 If A is a collection of AP's,

$$Z(A) \supseteq \langle A, D \rangle$$

and no proper subcollection of A has this property, we say that A is a *minimal covering* of $\langle A, D \rangle$.

If A is such that each element of $\langle A, D \rangle$ belongs to exactly one AP in A we say that A is an *exact covering* of $\langle A, D \rangle$.

Corollary 2.12 If A^* is the reduction of a collection A via $\langle A, D \rangle$ then

(a) A covers the integers if and only if A^* covers $\langle A, D \rangle$.

(b) A is a minimal covering of $\langle A, D \rangle$ if and only if A^* is a regular covering system.

(c) A is an exact covering of $\langle A, D \rangle$ if and only if A^* is an exact covering system.

(d) $Z(A)$ includes $\langle A + iD : i = 0, \ldots, n-1 \}$ if and only if $Z(A^*)$ includes $\{0, \ldots, n-1\}$.

Proof: Immediate from theorem 2.10. □

In Chapter 5 we will be concerned with AP's having modulus bounded below. A disadvantage of the reduction construction is that, in general, the modulus of an AP decreases when the AP is reduced. The final bit of this

chapter introduces another method of transforming one collection of AP's into another. This transformation has some properties which are similar to those of the reduction technique, but it does not change the moduli of the AP's. We call this transformation T_p, where p is a prime number.

Definition 2.13 Let p be any prime and let $\langle a,p^\alpha d\rangle$ be an AP in which p does not divide d. We define the transformation T_p by

$$T_p(\langle a,p^\alpha d\rangle) = \langle b,p^\alpha d\rangle$$

where

$$\begin{aligned} b &\equiv a \pmod{p^\alpha} \\ pb &\equiv a \pmod{d}. \end{aligned} \tag{9}$$

Similarly we define a transformation on a collection A of AP's.

$$T_p(A) = \{T_p(\langle a,d\rangle) : \langle a,d\rangle \in A\}$$

Theorem 2.14 (a) Let p be any prime and let A be a collection of AP's. Then

$$Z(A) = \mathbb{Z}$$

if and only if

$$Z(T_p(A)) = \mathbb{Z}$$

(b) Further, A is an exact covering if and only if $T_p(A)$ is an exact covering.

Proof: (a) Let

$$P(A) = p^{\alpha}P$$

where p does not divide P. Let m be any integer, and find another integer n such that

$$\begin{aligned} n &\equiv m \pmod{p^{\alpha}} \\ pn &\equiv m \pmod{P}. \end{aligned} \tag{10}$$

We will show that m belongs to an AP $\langle a, p^{\alpha}d\rangle$ if and only if n belongs to $T_p\langle a, p^{\alpha}d\rangle$, where p does not divide d.

$$\begin{aligned} & m \in \langle a, p^{\alpha}d\rangle \\ \Leftrightarrow \quad & m \equiv a \pmod{p^{\alpha}}, \\ & m \equiv a \pmod{d} \\ \Leftrightarrow \quad & n \equiv a \pmod{p^{\alpha}}, \\ & pn \equiv a \pmod{d} \\ \Leftrightarrow \quad & n \in T_p(\langle a, p^{\alpha}d\rangle. \end{aligned}$$

Since (10) describes a 1-1 and onto mapping from $\mathbb{Z}_{P(A)}$ to $\mathbb{Z}_{P(A)}$ it follows that each integer belongs to some AP in A if and only if each integer belongs to an AP in $T_p(A)$.

(b) It further follows that each integer belongs to exactly one AP in A if and only if each integer belongs to exactly one AP in $T_p(A)$. Thus A is an exact covering if and only if $T_p(A)$ is.

□

Theorem 2.15 If $\langle a,p^{\alpha}d\rangle$ is an AP, $p\nmid d$ and $\theta > \alpha \geqslant 0$, then $mp^{\theta} \in \langle a,p^{\alpha}d\rangle$ if and only if $mp^{\theta-1} \in T_p(\langle a,p^{\alpha}d\rangle)$.

Proof: Let

$$T_p(\langle a,p^{\alpha}d\rangle) = \langle b,p^{\alpha}d\rangle.$$

Then by (9),

$$mp^{\theta} \equiv a \pmod{d}$$

if and only if

$$mp^{\theta-1} \equiv b \pmod{d}.$$

Also by (9) and the hypothesis $\theta > \alpha$,

$$mp^{\theta} \equiv a \pmod{p^{\alpha}}$$

if and only if

$$mp^{\theta-1} \equiv b \pmod{p^{\alpha}}.$$

The theorem then follows. □

CHAPTER 3

REGULAR COVERING SYSTEMS

In this chapter we will obtain lower bounds for the number of AP's in a regular covering system, these bounds being in term of numbers such as $P(A)$, (see notation 1.1) which can be associated with the system. Since any exact covering system is also regular these results will also apply to exact covering systems. Before describing our results we will review their historical background.

Recall that in Chapter 1 we defined the following function. Let n be a positive integer with prime factorisation

$$n = \prod_{i=1}^{t} p_i^{\alpha_i},$$

we then define

$$f(n) = \sum_{i=1}^{t} \alpha_i (p_i - 1).$$

We note that $f(n)$ is completely additive.

In 1966 Mycielski and Sierpinski [16] conjectured that if A is an exact covering system, $\langle a,d \rangle$ belongs to A, then

$$|A| \geq f(d) + 1. \qquad (1)$$

This was proved by Znam [24] in 1966. Three years later [25] he proved the stronger result that if A covers the integers, $\langle a,d\rangle$ belongs to A and is disjoint from the other AP's in A then (1) still holds. In 1975 [26] he strengthened the result still further. He defined an AP in A as *essential* if

$$Z(A) = \mathbb{Z}$$
$$Z(A/\langle a,d\rangle) \neq \mathbb{Z},$$

and showed that $\langle a,d\rangle$ need only be essential in A for (1) to hold.

In another paper [24] he made the following conjecture.

If A is an exact covering system then

$$|A| \geqslant f(P(A)) + 1. \tag{2}$$

This was proven by Korec [13] in 1974. In 1975 Znam [26] conjectured that A need only be regular, not necessarily exact, for (2) to hold.

Our main result in this chapter, theorem 3.4, is the following. If A is a regular covering system, D is a proper divisor of $P(A)$, then

$$|\{\langle a,d\rangle \in A : d \not| D\}| \geqslant f(P(A)/D) + 1.$$

Znam's second conjecture is proved in corollary 3.5 of this theorem, and an extension of Znam's result about essential AP's is proved in corollary 3.6.

Another important theorem of this chapter is theorem 3.1 below. It extends the results of Billick and Edgar

mentioned in the last chapter and provides us with two corollaries. The first of these is used in the proof of theorem 3.4 and the second will be used in Chapter 5.

The final result of the chapter gives a lower bound on the cardinality of a collection of AP's that does not cover the integers. The bound is in terms of the least number P such that there exists an AP $\langle a,P\rangle$ which is disjoint from the AP's in the collection. The result will be used in Chapter 7.

Theorem 3.1 Suppose A is regular, $\langle a,d\rangle \in A$ and p^{α} is the highest power of a prime p which divides d. Then,

(i) for $1 \leqslant k \leqslant \alpha$ A has a subcollection A_k where

$$A_k = \{\langle a_i^{(k)}, d_i^{(k)}\rangle : 1 \leqslant i \leqslant p-1\}$$

such that for each i satisfying $1 \leqslant i \leqslant p-1$,

$$p^k \mid d_i^{(k)}$$

$$a_i^{(k)} \equiv a \pmod{p^{k-1}}$$

$$\frac{a_i^{(k)} - a}{p^{k-1}} \equiv i \pmod{p}.$$

(ii) The $\alpha(p-1)$ AP's $\langle a_i^{(k)}, d_i^{(k)}\rangle$ are pairwise disjoint, and each is disjoint from $\langle a,d\rangle$.

Proof: (i) We prove the result for an arbitrary value of k.

Let C be a minimal subcollection of A such that C covers $\langle a,p^{k-1}\rangle$ and let C^* be the reduction of C via

$\langle a,p^{k-1}\rangle$, as in definition 2.7 so that, by (b) of corollary 2.12, C^* is a regular covering system. Now $\langle a,d\rangle$ is a subset of $\langle a,p^{k-1}\rangle$ so the regularity of A implies that $\langle a,d\rangle$ belongs to C. By remark 2.9 $\langle 0,d/p^{k-1}\rangle$ belongs to C^*. Since p divides d/p^{k-1} corollary 2.6 implies that C^* contains a further $p-1$ AP's $\langle a_1^*,d_1^*\rangle,\ldots,$ $\langle a_{p-1}^*,d_{p-1}^*\rangle$ such that $\{0,a_1^*,\ldots,a_{p-1}^*\}$ is a complete residue system modulo p and that each d_i^* is divisible by p.

For each i, let $\langle a_i^{(k)},d_i^{(k)}\rangle$ be the AP of which $\langle a_i^*,d_i^*\rangle$ is the reduction. Then by definition 2.7,

$$d_i^* = \frac{d_i^{(k)}}{(p^{k-1},d_i^{(k)})} .$$

Since p divides d_i^* this implies that p^k divides $d_i^{(k)}$. Now $\langle a_i^{(k)},d_i^{(k)}\rangle$ intersects $\langle a,p^{k-1}\rangle$ so by (a) of theorem 2.1.

$$a_i^{(k)} \equiv a \pmod{p^{k-1}}$$

and by remark 2.9

$$a_i^* \equiv \frac{a_i^{(k)} - a}{p^{k-1}} \pmod{p} .$$

Since a_i^* runs through a reduced residue system modulo p we can, by appropriate ordering, ensure that,

$$\frac{a_i^{(k)} - a}{p^{k-1}} \equiv i \pmod{p} .$$

(ii) We prove this part by contradiction. Suppose $\langle a_i^{(k)}, d_i^{(k)} \rangle$ intersects $\langle a_{i'}^{(k')}, d_{i'}^{(k')} \rangle$ where $k' \geq k$ so that p^k divides $(d_i^{(k)}, d_{i'}^{(k')})$. Then by (a) of theorem 2.1

$$a_i^{(k)} \equiv a_{i'}^{(k')} \pmod{p^k}$$

and so

$$\frac{a_i^{(k)} - a}{p^{k-1}} \equiv \frac{a_{i'}^{(k')} - a}{p^{k-1}} \pmod{p} .$$

The left hand side here is congruent to i and the right to 0 if k' exceeds k and to i' if k' equals k. The first alternative is impossible since i belongs to the reduced residue system modulo p, and the second implies that the two AP's are identical.

Similarly $\langle a_i^{(k)}, d_i^{(k)} \rangle$ intersecting $\langle a, d \rangle$ would imply

$$a_i^{(k)} \equiv a \pmod{p^k}$$

and thus

$$\frac{a_i^{(k)} - a}{p^{k-1}} \equiv 0 \pmod{p} .$$

This is a contradiction since the left is congruent to i modulo p. □

Corollary 3.2 With A as in the theorem, let n and β be integers satisfying

$$0 \leq n \leq p^{\alpha}$$

$$0 < \beta \leq \alpha$$

and

$$\mathcal{B} = \bigcup_{s=1}^{n} \langle b_s, p^\alpha \rangle$$

where the numbers b_s are distinct modulo p^α. Then

$$|\{\langle a,\delta\rangle \in A : p^\beta | \delta,\ \langle a,\delta\rangle \cap \mathcal{B} = \phi\}| \geq (\alpha-\beta+1)(p-1) + 1 - n.$$

Proof: By the theorem, A contains the $(p-1)(\alpha-\beta+1) + 1$ AP's

$$\langle a_i^{(k)}, d_i^{(k)} \rangle \quad \text{for} \quad k = \beta,\ldots,\alpha \ , \quad i = 1,\ldots,p-1$$

and

$$\langle a,d \rangle .$$

Each of these has modulus divisible by p^β. Now suppose both $\langle a_i^{(k)}, d_i^{(k)} \rangle$ and $\langle a_{i'}^{(k')}, d_{i'}^{(k')} \rangle$ intersect $\langle b_s, p^\alpha \rangle$ and that $k' \geq k$. Then by (e) of theorem 2.1

$$a_i^{(k)} \equiv a_{i'}^{(k')} \pmod{p^k} ,$$

which leads to a contradiction as in part (ii) of the theorem. Similarly no $\langle a_i^{(k)}, d_i^{(k)} \rangle$ will intersect $\langle a, p^\alpha \rangle$, which contains $\langle a,d \rangle$. Thus at most n of our AP's will intersect AP's in $\mathcal{B}$ leaving at least $(\alpha-\beta+1)(p-1) + 1 - n$ non-intersecting AP's.

□

Corollary 3.3 If A is a collection of AP's and p is a prime such that for some i and j,

$$Z(A) \supseteq \langle ip^{\alpha-1}, p^\alpha \rangle$$

$$Z(A) \not\supseteq \langle jp^{\alpha-1}, p^\alpha \rangle$$

then A contains an AP $\langle a,d \rangle$ with $p^\alpha | d$ and

$$a \equiv ip^{\alpha-1} \pmod{p^\alpha} .$$

Proof: We first form a collection of AP's

$$B = \{\langle n, p^\alpha\rangle \ : \ 1 \leqslant n \leqslant p^\alpha, \ \ Z(A) \not\equiv \langle n, p^\alpha\rangle\}.$$

We then have

$$\langle ip^{\alpha-1}, p^\alpha\rangle \notin B, \tag{3}$$

and

$$Z(A \cup B) = \mathbb{Z}.$$

Now let C be a regular subcollection of $A \cup B$. It is clear that $\langle jp^{\alpha-1}, p^\alpha\rangle$ belongs to C, so by theorem 3.1 C contains an AP $\langle a,d\rangle$ with

$$p^\alpha | d$$

$$a \equiv jp^{\alpha-1} \pmod{p^{\alpha-1}}$$

$$\frac{a - jp^{\alpha-1}}{p^{\alpha-1}} \equiv i - j \pmod{p}.$$

The two congruences are equivalent to

$$a \equiv ip^{\alpha-1} \pmod{p^\alpha}.$$

By (3) above $\langle a,d\rangle$ does not belong to B, so it belongs to A and we are done. □

Theorem 3.4 If A is a regular covering system, D is a positive integer which divides $P(A)$ and D does not equal $P(A)$, then

$$|\{\langle a,d\rangle \in A \ : \ d \not| D\}| \geqslant 1 + f(P(A)/D),$$

where $P(A)$ and f are defined in notation 1.1.

Proof: We prove the theorem by induction on $\nu(P(A))$, the number of distinct prime divisors of $P(A)$.

If $\nu(P(A))$ equals 1 then

$$P(A) = p^{\alpha}, \quad D = p^{\beta}, \quad 0 \leq \beta < \alpha$$

where p is a prime. We then have

$$|\{<a,d> \in A : d \not| p^{\beta}\}| = |\{<a,d> \in A : p^{\beta+1} | d\}| .$$

By corollary 3.2 this is not less than

$$(\alpha - (\beta+1) + 1)(p-1) + 1 = f\left(\frac{p^{\alpha}}{p^{\beta}}\right) + 1 .$$

This shows that the theorem holds when $\nu(P)$ equals 1.

To continue the induction suppose that the theorem holds for $\nu(P)$ not exceeding n. Let A be regular and let $P(A)$ be $p^{\alpha}P$, where p is a prime not dividing P and $\nu(P)$ equals n, so that $\nu(P(A)) = n + 1$. We will write the AP's in A in the form $<a,p^{\gamma}d>$ where p does not divide d. We must find a lower bound for

$$|\{<a,p^{\gamma}d> \in A : p^{\gamma}d \not| p^{\beta}D\}|$$

where p does not divide D.

We now introduce some notation. For each residue class s modulo p^{α} let A_s be a minimal subcollection of A that covers $<s,p^{\alpha}>$. It is clear that such a subcollection exists. We then set

$P_s = \ell cm\{d : \langle a,p^\gamma d\rangle \in A_s\}$

$R_o = D,$

$R_s = \ell cm\ \{R_{s-1}, P_s\},$

$D_s = (R_{s-1}, P_s),$

$Q_s = \{\langle a,p^\gamma d\rangle \in A_s : d \not| D_s\}, \quad \text{for} \quad s = 1,\ldots,p^\alpha.$

We remark that:

$$\frac{P_s}{D_s} = \frac{R_s}{R_{s-1}} \quad \text{for} \quad s = 1,\ldots,p^\alpha, \tag{4}$$

$$R_{p^\alpha} = P, \tag{5}$$

Q_s is empty if $D_s = P_s$, (6)

$$Q_s = \{\langle a,p^\gamma d\rangle \in A_s : d | R_s, \quad d \not| R_{s-1}\}. \tag{7}$$

It is clear from the last remark and from the definition of R_s that the collections Q_s are pairwise disjoint.

Claim: If D_s does not equal P_s,

$$|Q_s| \geqslant f\left(\frac{P_s}{D_s}\right) + 1 \tag{8}$$

Proof of Claim: Since A_s is a minimal covering of $\langle s,p^\alpha\rangle$ we may reduce it to get a regular covering A_s^*. Any AP $\langle a,p^\alpha d\rangle$ in A_s will be reduced, as in definition 2.7, to an AP of the form $\langle a^*,d\rangle$. Since $D_s | P_s$ and $\nu(P_s)$ is at most n, it follows from the induction hypothesis that if D_s does not equal P_s,

$$|Q_s| = |\{<a^*,d> \in A_s^* : d \not| D_s\}|$$

$$\geqslant f\left(\frac{P_s}{D_s}\right) + 1. \qquad \square$$

We now obtain a lower bound for the cardinality of the set $\{<a,p^\gamma d> \in A : p^\gamma d \not| p^\beta D\}$. We note that

$$p^\gamma d \not| p^\beta D \Rightarrow p^{\beta+1} | p^\gamma \quad \text{or} \quad d \not| D$$

and

$$\bigcup_{s=1}^{p^\alpha} A_s = A.$$

Therefore the cardinality equals

$$|\left(\bigcup_{s=1}^{p^\alpha} \{<a,p^\gamma d> \in A_s : d \not| D\}\right) \cup \{<a,p^\gamma d> \in A : p^{\beta+1} | p^\gamma\}|.$$

Each collection in the first union contains a subcollection

$$\{<a,p^\gamma d> \in A_s : d \not| D_s\} = Q_s,$$

so the required cardinality is at least

$$|\left(\bigcup_{s=1}^{p} Q_s\right) \cup \{<a,p^\gamma d> \in A : p^{\beta+1} | p^\gamma\}|$$

$$\geqslant \sum_{\substack{s=1 \\ P_s \neq D_s}}^{p^\alpha} |Q_s| + |\{<a,p^\gamma d> \in A \setminus \bigcup_{\substack{s=1 \\ P_s \neq D_s}}^{p} A_s : p^{\beta+1} | p^\gamma\}|. \qquad (9)$$

By (4) to (8) and the additivity of f,

$$\sum_{\substack{s=1\\ P_s \neq D_s}}^{p^\alpha} |Q_s| \geqslant \sum_{\substack{s=1\\ P_s \neq D_s}}^{p^\alpha} f\left(\frac{P_s}{D_s}\right) + \sum_{\substack{s=1\\ P_s \neq D_s}}^{p^\alpha} 1$$

$$= \sum_{s=1}^{p^\alpha} f\left(\frac{R_s}{R_{s-1}}\right) + \sum_{\substack{s=1\\ P_s \neq D_s}}^{p^\alpha} 1 = f\left(\frac{P}{D}\right) + \sum_{\substack{s=1\\ P_s \neq D_s}}^{p^\alpha} 1. \quad (10)$$

We now consider the second term in (9). We put

$$B = \bigcup_{\substack{s=1\\ P_s \neq D_s}}^{p} \langle s, p^\alpha \rangle$$

and note that if the intersection of $\langle a, p^\gamma d\rangle$ and $\langle s, p^\alpha\rangle$ is empty then $\langle a, p^\gamma d\rangle$ does not belong to Q_s, so the second term in (9) is at least

$$|\{\langle a, p^\gamma d\rangle \in A : \langle a, p^\gamma d\rangle \cap B = \phi, \ p^{\beta+1} | p^\gamma\}|.$$

By corollary 3.2 this is at least

$$\left(\alpha - (\beta+1) + 1\right)(p-1) + 1 - \sum_{\substack{s=1\\ P_s \neq D_s}}^{p^\alpha} 1 = f\left(\frac{p^\alpha}{p^\beta}\right) + 1 - \sum_{\substack{s=1\\ P_s \neq D_s}}^{p^\alpha} 1. \quad (11)$$

On adding the right hand sides of (10) and (11) we obtain the required lower bound. That is,

$$|\{\langle a, p^\gamma d\rangle \in A : p^\gamma d \not| p^\beta D\}|$$

$$\geqslant f\left(\frac{P}{D}\right) + \sum_{\substack{s=1\\ P_s \neq D_s}}^{p^\alpha} 1 + f\left(\frac{p^\alpha}{p^\beta}\right) + 1 - \sum_{\substack{s=1\\ P_s \neq D_s}}^{p^\alpha} 1 = f\left(\frac{p^\alpha P}{p^\beta D}\right) + 1.$$

Thus the theorem holds when the least common multiple of the moduli has $n+1$ distinct prime factors and the theorem is proven by induction. □

The first corollary to this theorem proves Znam's 1975 conjecture [26].

Corollary 3.5 If A is a regular covering system

$$|A| \geqslant f(P(A)) + 1.$$

Proof: If $P(A)$ does not equal 1 we obtain the result immediately on setting D equal to 1 in the theorem. If $P(A)$ equals 1 then A must be $\{<0,1>\}$ and the result still holds. □

Recall that an AP $<a_o,d_o>$ is essential in A if A covers the integers but $A\backslash<a_o,d_o>$ does not. The next corollary extends theorem 1 of [25].

Corollary 3.6 If $<a_o,d_o>$ is essential in A, then

$$|\{<a,d> \in A : (d,d_o) > 1\}| \geqslant f(d_o) + 1.$$

Let A^* be a regular subcollection of A. It is clear that $<a_o,d_o>$ belongs to A^* and so d_o divides $P(A^*)$. By the theorem we then have

$$\begin{aligned} &|\{<a,d> \in A : (d,d_o) > 1\}| \\ &\geqslant |\{<a,d> \in A^* : d \nmid P(A^*)/d_o\}| \\ &\geqslant f(d_o) + 1. \end{aligned}$$

□

Theorem 3.7 The bounds in corollaries 3.5 and 3.6 are best possible.

Proof: We show that for any positive integer n there exists a regular covering A with

$$P(A) = n$$

and

$$|A| = f(n) + 1.$$

This will establish that corollary 3.5 is best possible. Furthermore we will construct such a collection which includes $<0,n>$, and so with $<a_o,d_o>$ set equal to $<0,n>$ we obtain equality in corollary 3.6.

If n equals 1 we set $A = \{<0,1>\}$ which is satisfactory. For n greater than 1, suppose n has prime factorisation

$$n = \prod_{i=1}^{t} p_i^{\alpha_i}.$$

Then let

$$A = \bigcup_{i=1}^{t} \bigcup_{j=1}^{\alpha_i} \bigcup_{k=1}^{p_i-1} \{<kp_i^{j-1}, p_i^j>\} \cup <0,n>.$$

We claim that A covers the integers. To see this note that

$$\bigcup_{k=1}^{p_i-1} <kp_i^{j-1}, p_i^j> = <0,p_i^{j-1}> \setminus <0,p_i^j>.$$

So,

$$\bigcup_{j=1}^{\alpha_i} \bigcup_{k=1}^{p_i-1} <kp_i^{j-1}, p_i^j> = \bigcup_{j=1}^{\alpha_i} <0,p_i^{j-1}> \setminus <0,p_i^j>$$

$$= \mathbb{Z} \setminus <0,p_i^{\alpha_i}>$$

We then have,

$$\bigcup_{i=1}^{t} \bigcup_{j=1}^{\alpha_i} \bigcup_{k=1}^{p_i-1} <kp_i^{j-1}, p_i^j> = \bigcup_{i=1}^{t} (\mathbb{Z} \setminus <0,p_i^{\alpha_i}>)$$

$$= \mathbb{Z} \setminus \bigcap_{i=1}^{t} <0,p_i^{\alpha_i}>$$

$$= \mathbb{Z} \setminus <0,n>.$$

So that A covers the integers. It is clear that $|A|$ equals $f(n) + 1$ as required.

It remains to show that if any AP is omitted from A the resulting collection will not cover the integers. If $<0,n>$ is omitted then 0 will not be covered. If we omit $<kp_i^{j-1}, p_i^j>$ for some choice for i, j and k then it is easy to check that no term in the intersection

$$<kp_i^{j-1}, p_i^j> \cap <0, \prod_{\substack{i=1 \\ i \neq j}}^{t} p_i^{\alpha_i}>$$

is covered. This completes the proof. □

The last theorem of this chapter concerns collections of AP's which do not cover the integers. We use the following function which was introduced in Chapter 1.

Notation 3.8 If P has prime factorisation

$$P = \prod_{i=1}^{t} p_i^{\alpha_i} \tag{12}$$

then

$$g(P) = \sum_{i=1}^{t} \left((\alpha_i - 1)(p_i - 1) + 1\right).$$

Theorem 3.9 If A is a collection of AP's such that

$$Z(A) \neq \mathbb{Z}$$

and P is the least integer for which there exists an AP $\langle a,P\rangle$ such that

$$Z(A) \cap \langle a,P\rangle = \phi$$

then

$$|A| \geqslant g(P).$$

Proof: The theorem clearly holds when $A = \phi$ since then $\langle a,P\rangle = \langle 0,1\rangle$, $g(P) = 0$. Suppose $A \neq \phi$. Without loss of generality we can assume $a = 0$. Let P have prime factorisation as in display (12). Now fix some p_i and for convenience put

$$p = p_i , \qquad \alpha = \alpha_i$$

For each of the $g(p^{\alpha})$ ordered pairs $\{\beta,k\}$ in the set

$$\{\{\beta,k\} : \beta \in [1,\alpha-1], k \in [1,p-1]\} \cup \{\alpha-1,0\}\} \tag{13}$$

we have, by the minimality of P,

$$Z(A) \cap (\langle 0,P/p^{\alpha}\rangle \cap \langle kp^{\alpha-1},p^{\beta}\rangle) \neq \phi ,$$

since the intersection of the two AP's is an AP with modulus less than P. Thus for each ordered pair $\{\beta,k\}$ A contains an AP, say $\langle A,p^{\gamma}D\rangle$ with $p\nmid D$, such that

$$\langle A,p^{\gamma}D\rangle \cap (\langle 0,P/p^{\alpha}\rangle \cap \langle kp^{\beta-1},p^{\beta}\rangle) \neq \phi. \tag{14}$$

By (a) of theorem 2.1 we then have

$$A \equiv 0 \quad (\mathrm{mod}(p^{\gamma}D,P/p^{\alpha}))$$

and

$$A \equiv kp^{\beta-1} \quad (\mathrm{mod}(p^{\gamma}D,p^{\beta})).$$

That is,

$$A \equiv 0 \quad (\mathrm{mod}(D,P/p^{\alpha})) \tag{15}$$

and

$$A \equiv kp^{\beta-1} \quad (\mathrm{mod}(p^{\gamma},p^{\beta})). \tag{16}$$

But we know $\langle 0,P\rangle$ is disjoint from $Z(A)$ so we must have

$$\langle A,p^{\gamma}D\rangle \cap \langle 0,P\rangle = \phi.$$

Part (a) of theorem 2.1 then implies

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

Since $\langle 0,(p^{\gamma}D,P)\rangle$ is the intersection of $\langle 0,(p^{\gamma},p^{\alpha})\rangle$ and $\langle 0,(D,P/p^{\alpha})\rangle$ this implies that one of the following holds.

$$A \not\equiv 0 \quad (\mathrm{mod}(p^{\gamma},p^{\alpha})) \tag{17}$$

$$A \not\equiv 0 \quad (\mathrm{mod}(D,P/p^{\alpha})).$$

By comparison with (15) we see that the first of these must be true and by comparing (16) and (17) we see that $\gamma \geq \beta$. Thus $\langle A,p^{\gamma}D\rangle$ has the form

$$<\ell(D,P/p^{\alpha}),D> \cap <kp^{\beta-1} + mp^{\beta},p^{\gamma}> \qquad (18)$$

for some ℓ and m, and with $\gamma \geq \beta$. We get such an AP for each pair $\{\beta,k\}$ allowed by (13) and it is not hard to see that they are disjoint, (each is a subset of $<kp^{\beta-1},p^{\beta}>$).

Thus we have $g(p^{\alpha})$ AP's in A satisfying (18) for each prime in the set $\{p_1,p_2,\ldots,p_t\}$. This gives a total of $g(P)$ AP's. Our final step is to show that AP's of the form in (18) but corresponding to different values of p are distinct.

Suppose not. Then there is an AP in A, $<A,p^{\gamma}D>$ say, which by (14) satisfies

$$<A,p^{\gamma}D> \cap <O,P/p^{\alpha}> \neq \phi$$

for some prime p, and for some prime p_j distinct from p satisfies

$$<A,p^{\gamma}D> \cap <O,P/p_j^{\alpha i}> \neq \phi$$

But

$$<O,P/p^{\alpha}> \cap <O,P/p_j^{\alpha i}> = <O,P>$$

so by theorem 2.2 $<A,p^{\gamma}D>$ intersects $<O,P>$, contrary to the assumptions of the theorem. This shows that AP's associated with different primes p_i are distinct. AP's corresponding to the same prime p_i are disjoint (and therefore distinct) by the remarks following display (18). Thus A contains at least $g(P)$ AP's and we are done.

□

CHAPTER 4

EXACT COVERING SYSTEMS

In notation 1.1 we defined an exact covering system (henceforth an ECS) as a collection of AP's which covers the integers and whose members are pairwise disjoint. The greater structure of an ECS compared with a regular covering system makes this type of covering system easier to investigate. We begin this chapter with two old results about such systems.

Theorem 4.1 If A is an ECS where

$$A = \{<a_i,d_i> : i = 1,\ldots,t\}$$

then

$$\sum_{i=1}^{t} \frac{1}{d_i} = 1.$$

Proof: Each AP $<a_i,d_i>$ covers exactly $P(A)/d_i$ residue classes modulo $P(A)$. Since these AP's are pairwise disjoint the total number of residue classes modulo $P(A)$ included in $Z(A)$ is

$$\sum_{i=1}^{t} P(A)/d_i.$$

Since $Z(A) = \mathbb{Z}$ this sum must equal $P(A)$ which gives the required result. □

This theorem will be used in the proof of corollary 4.16.

Our main results in this chapter concern ECS(M)'s which we define as follows.

Definition 4.2 An ECS in which each modulus occurs at most M times is called an ECS(M)

Our second theorem is due to Davenport, Mirsky, Newman and Rado [11]

Theorem 4.3 The only ECS(1) is $\{<0,1>\}$.

Proof: Suppose A is an ECS(1) where

$$A = \{<a_i,d_i> : i = 1,\ldots,t\}$$

and

$$0 < d_1 < d_2 < \ldots < d_t.$$

It is not hard to see that if z is a complex number with absolute value less than 1 then the a_i's and d_i's must satisfy the identity

$$1/(1-z) = \sum_{i=1}^{t} z^{a_i}/(1-z^{d_i}). \qquad (1)$$

Let z_o be a primitive d_t^{th} root of unity, and let z approach z_o. If d_t does not equal 1, so that z_o does not equal 1, the absolute value of the right hand side of (1) approaches infinity while the left hand side remains bounded. This contradiction implies that $d_t = 1$, and so we must have $A = \{<0,1>\}$.

□

Several authors (see [1] and [19]) have commented that no proof of this result is known that does not use

complex numbers. One aim of this chapter is to remedy this deficiency. More generally we will be concerned with characterising ECS(M)'s for arbitrary M.

For a given M we may ask questions analogous to those asked by Erdös about regular covering systems with distinct moduli. That is, we ask

I For a given M, do there exist ECS(M)'s with all moduli arbitrarily large?

II For a given M, do there exist ECS(M)'s with all moduli relatively prime to some given set of primes?

We will answer the first of these questions in the negative (see corollary 4.16). As a partial answer to the second question we give a condition that must be satisfied by the set of primes dividing the moduli of an ECS(M). This condition is given in theorem 4.12 which we state now.

Theorem 4.12 If A is an ECS(M) and $p_1 < p_2 < \ldots < p_t$ are the distinct prime divisors of P(A), then

$$p_t \leq M \prod_{i=1}^{t-1} p_i/(p_i-1).$$

This extends work done by Burshtein ([2],[3]) on a special type of ECS called a naturally exact covering system. The idea of such a collection was invented by Znam [27] who defined them in terms of rooted trees. We use here an alternative definition due to Korec [14].

Definition 4.4 An ECS A is a naturally exact covering system (henceforth an NECS) if there exists a finite sequence of collections $A_0, A_1, \ldots, A_t$ such that

$$A_0 = \{<0,1>\}, \quad A_t = A$$

and for $i = 1,\ldots,t$ there is a prime p_i and an AP $<a_i,d_i>$ in A_i such that

$$A_{i+1} = \{A_i \setminus \{<a_i,d_i>\}\} \cup \{<a_i + jd_ip_i>: j = 1,\ldots,p\}.$$

Informally A_{i+1} is formed from A_i by partitioning one of the AP's in A_i into p_i AP's of equal modulus.

Example 4.5 If we set

$$\{a_1,d_1,p_1\} = \{0,1,2\}$$

and

$$\{a_2,d_2,p_2\} = \{0,2,3\}$$

we get

$$A_0 = \{<0,1>\}$$

$$A_1 = \{<0,2>,<1,2>\}$$

$$A_2 = \{<0,6>,<2,6>,<4,6>,<1,2>\}$$

A_0, A_1 and A_2 are NECS's.

Not all ECS's are NECS's as the following example, due to Porubsky [18], shows.

Example 4.6 The collection

$$\{<0,6>,<4,6>,<1,10>,<3,10>,<7,10>,<9,10>,<5,15>$$
$$<2,30>,<8,30>,<14,30>,<15,30>,<25,30>,<26,30>\}$$

is an ECS which is not an NECS. To see that it is not an NECS note that it contains no subcollection of AP's with equal moduli whose union is an AP.

The main result proved by Burshtein is the following (theorem 2.7 of [3]).

Theorem 4.7 If A is an NECS in which each modulus occurs at most M times and $p_1 < p_2 < \ldots < p_t$ are the distinct prime divisors of $P(A)$ then

$$p_t \leq M \prod_{i=1}^{t} p_i/(p_i-1)$$

Note that in our theorem 4.12 the product is over values of i from 1 to $t-1$ rather than 1 to t. This means theorem 4.12 is slightly stronger than theorem 4.7 even when we restrict our attention to NECS's. For instance, theorem 4.12 shows there is no ECS(2) whose moduli are divisible only by the primes 2 and 5. Burshtein's theorem does not forbid such collections.

We will now prove two lemmas which will be used in the proof of theorem 4.12. We then prove that theorem and derive some corollaries. In the final part of the chapter we make some comparisons between our results and one of the questions asked by Erdös which were mentioned in Chapter 1.

Lemma 4.8 If A is an ECS(M), $p^{\alpha} \| P(A)$ and A^* is the reduction (see definition 2.7) of A via $\langle a, p^{\alpha-1} \rangle$ for some integer a, then A^* is an ECS in which each modulus divisible by p occurs at most M times.

Proof: We know A^* is an ECS by part (c) of corollary 2.12, with $\langle a,p^{\alpha-1}\rangle$ in the role of $\langle A,D\rangle$. Now suppose $\langle b^*,pd^*\rangle$ in A^* is the reduction of an AP $\langle b,d\rangle$ in A. Then by definition 2.7

$$pd^* = d/(p^\alpha,d).$$

Since d cannot be divisible by a higher power of p than p^α we have

$$pd^* = d/p^{\alpha-1}.$$

Since there are at most M AP's in A with modulus d there are at most M in A^* with modulus pd^*. □

For the next lemma we need the following definition.

Definition 4.9 Let S be a collection of AP's. We say that an AP $\langle a,d\rangle$ is *maximal in* S if S covers $\langle a,d\rangle$ but S does not cover any AP $\langle a,\Delta\rangle$ where Δ is a proper divisor of d.

Remark 4.10 It follows that if S covers $\langle a,d\rangle$ then $d = \Delta d'$ where $\langle a,d'\rangle$ is maximal in S.

Lemma 4.11 Suppose S is a collection of AP's, each having modulus D.

(a) If $\langle a,d\rangle$ is covered by S then so is $\langle a,(d,D)\rangle$.

(b) If $\langle a,d\rangle$ is maximal in S then d divides D.

Proof: (a) It follows easily from theorem 2.1 (a) that if $\langle a,(d,D)\rangle$ intersects an AP $\langle A,D\rangle$, then so does $\langle a,d\rangle$.

Hence if $\langle a,(d,D)\rangle$ intersects an AP $\langle A,D\rangle$ not belonging to S, then so does $\langle a,d\rangle$. Thus if $\langle a,(d,D)\rangle$ is not covered by S, then neither is $\langle a,d\rangle$.

(b) If $\langle a,d\rangle$ is maximal then by part (a)

$$d = (D,d),$$

so D divides d as required. □

We are now ready to prove our main theorem. We recall from notation 1.2 that empty products equal 1.

Theorem 4.12 If A is an ECS(M) and $p_1 < p_2 < \cdots < p_t$ are the distinct prime divisors of $P(A)$ then

$$p_t \leqslant M \prod_{i=1}^{t-1} \frac{p_i}{p_i - 1} . \tag{2}$$

Proof: The proof is by contradiction. Suppose that A is an ECS(M) that does not satisfy (2) and that $p_t^{\alpha} \| P(A)$.

Let $\langle a_o, p_t^{\alpha} d\rangle$ belong to A and let A^* be the reduction of A via $\langle a_o, p_t^{\alpha-1}\rangle$. It follows from definition 2.7 and lemma 4.8 that $p_t \| P(A^*)$ and each modulus that appears in A^* and is divisible by p_t occurs at most M times in A^*.

We now set

$$B = \{\langle a,d\rangle \quad A^* : p_t \nmid d\}$$

$$C = \{\langle a,d\rangle \quad A^* : p_t \mid d\}$$

$$D = P(B).$$

From the remarks above we see that

$$A^* = B \cup C, \quad C \neq \phi, \quad p_t \nmid D \tag{3}$$

and each modulus appearing in $\mathcal{C}$ occurs at most M times. We note that by theorem 2.1 (c) each residue class mod D is either covered by an AP in $\mathcal{B}$ and so covered by $\mathcal{B}$ or else is disjoint from all AP's in $\mathcal{B}$. Let

$$\mathcal{S} = \{\langle A,D\rangle : \langle A,D\rangle \text{ is disjoint from } \mathcal{B}\}$$

and note that this is nonempty since $\mathcal{C}$ is nonempty and A^* is exact.

By remark 4.10 if $\langle a,d\rangle$ is any AP covered by $\mathcal{S}$ then

$$d = \Delta d' \tag{4}$$

where $\langle a,d'\rangle$ is maximal in $\mathcal{S}$, and by part (b) of lemma 4.11

$$d' \mid D. \tag{5}$$

We now let

$$\mathcal{D} = \{d_1, d_2, \ldots, d_n\}$$

by the set of distinct moduli of maximal AP's covered by $\mathcal{S}$. $\mathcal{D}$ is clearly nonempty.

At this point we outline the ideas of the proof. We will use the set $\mathcal{D}$ to obtain a lower bound on the number of residue classes modulo $p_t D$ that are covered by $\mathcal{S}$. These must be covered by AP's in $\mathcal{C}$, and such AP's have moduli satisfying (4) and (5) and other conditions stated in the first paragraph of this proof. We will introduce a number P which is a large multiple of D and use these conditions to obtain an upper bound on the number of residue classes modulo $p_t D$ that are covered by $\mathcal{C}$, this bound also being given in terms of the set $\mathcal{D}$. Each residue class modulo D is the

disjoint union of $p_t P/D$ residue classes modulo $p_t P$ so the two bounds may be compared. Our contradiction will be obtained when we show that the lower bound exceeds the upper bound.

We now obtain our lower bound. By the definition of $\mathcal{D}$ there exists a collection of AP's

$$\{<a_i,d_i> : i = 1,\ldots,n\}$$

whose union is covered by S. By applying lemma 2.3 to this collection we obtain

$$|S| \geqslant D\left\{ \sum_{1\leqslant i\leqslant n} \frac{1}{d_i} - \sum_{1\leqslant i<j\leqslant n} \frac{1}{[d_i,d_j]} + \ldots \right\}$$

It follows that the number of residue classes mod $p_t D$ *not* covered by $\mathcal{B}$ is at least

$$p_t D\left\{ \sum_{1\leqslant i\leqslant n} \frac{1}{d_i} - \sum_{1\leqslant i<j\leqslant n} \frac{1}{[d_i,d_j]} + \ldots \right\} \qquad (6)$$

and these must be covered by AP's in $\mathcal{C}$.

We now turn our attention to these AP's, recalling that each has modulus divisible by p_t but not by p_t^2 and each is covered by S. By (4) above, the definition of $\mathcal{C}$ and our observation (3) that p_t does not divide D (so that p_t does not divide any d_i) each AP in $\mathcal{C}$ has the form

$$<a,p_t d_i \Delta> \qquad (7)$$

where the prime factors of Δ come from the set $\{p_1,p_2,\ldots,p_{t-1}\}$ and d_i belongs to $\mathcal{D}$.

We now define

$$P = \left(\prod_{i=1}^{t-1} p_i \right)^N$$

where N is chosen sufficiently large so that

$$D \mid P,$$

$$\langle a, p_t d_i \Delta \rangle \in C \Rightarrow d_i \Delta \mid P,$$

and P satisfies inequality (10) below. The number of residue classes modulo $p_t P$ that are covered by one AP having this form is

$$\frac{p_t P}{p_t d_i \Delta} = \frac{P}{d_i \Delta} . \tag{8}$$

The moduli of the AP's occurring in C have the form $p_t d_i \Delta$ where d_i divides P and d_i belongs to $\mathcal{D}$. Each such modulus appears in at most M of the AP's in C, and the number of residue classes modulo $p_t P$ covered by such an AP is given by (8). To obtain an upper bound on the number of such residue classes covered by C we may suppose that each allowable modulus appears M times. We therefore sum the expression (8) over all allowable moduli, then multiply the total by M. In doing this we use inclusion-exclusion, summing over the indices i and noting that an allowable modulus may be divisible by more than one element of $\mathcal{D}$.

If there were one AP having modulus $p_t d_i \Delta$ for each i and Δ such that $d_i \Delta$ divides P then the number of residue classes modulo $p_t P$ covered would be

$$\sum_{1\leq i\leq n} |\{\text{classes covered by AP's with modulus divisible by } d_i\}|$$

$$- \sum_{1\leq i\leq j\leq n} |\{ \ldots \quad \text{with modulus divisible by } [d_i,d_j]\}|$$

$$+ \ldots$$

$$= \sum \frac{P}{d_i} \sum_{\Delta | P/d_i} \frac{1}{\Delta} - \sum_{1\leq i\leq j\leq n} \frac{P}{[d_i,d_j]} \sum_{\Delta | P/[d_i,d_j]} \frac{1}{\Delta} + \ldots$$

Here and in the rest of this chapter square brackets denote lowest common multiple. On multiplying this expression by M we obtain the required upper bound. That is, the number of residue classes modulo $p_t P$ covered by $\mathcal{C}$ is at most

$$MP\left\{ \sum \frac{1}{d_i} \sum_{\Delta | P/d_i} \frac{1}{\Delta} - \sum \frac{1}{[d_i,d_j]} \sum_{\Delta | P/[d_i,d_j]} \frac{1}{\Delta} + \ldots \right\} \qquad (9)$$

We now make our final requirement on the size of N. By hypothesis, inequality (2) is not satisfied so

$$M \prod_{i=1}^{t-1} \frac{p_i}{p_i - 1} = p_t - \delta \qquad (10)$$

for some $\delta > 0$. Now define a positive number ε by:

$$\varepsilon = \frac{1}{2}\frac{\delta}{M} \frac{\left\{ \sum \frac{1}{d_i} - \sum \frac{1}{[d_i,d_j]} + \ldots \right\}}{\left\{ \sum \frac{1}{[d_i,d_j]} + \sum \frac{1}{[d_i,d_j,d_k,d_l]} + \ldots \right\}} \qquad (11)$$

where the sum in the denominator is over all subsets of $\mathcal{D}$ with even cardinality, and the numerator is positive by lemma 2.3.

Now as $N \to \infty$,

$$\sum_{\Delta | P/[d_1,\ldots,d_n]} \frac{1}{\Delta} \to \left[1 + \frac{1}{p_1} + \frac{1}{p_1^2} + \ldots\right]\left[1 + \frac{1}{p_2} + \frac{1}{p_2^2} + \ldots\right] \cdots \left[1 + \frac{1}{p_{t-1}} + \ldots\right]$$

$$= \prod_{i=1}^{t-1} \frac{p_i}{p_{i-1}} .$$

The left hand side is approaching the limit from below so we may choose N sufficiently large so that

$$\prod_{i=1}^{t-1} \frac{p_i}{p_i - 1} - \varepsilon < \sum_{\Delta | P/[d_1,\ldots,d_n]} \frac{1}{\Delta} < \pi \frac{p_i}{p_i - 1} \tag{12}$$

It follows that

$$\prod_{i=1}^{t-1} \frac{p_i}{p_i - 1} - \varepsilon < \sum_{\Delta | P/[d_{i_1},\ldots,d_{i_s}]} \frac{1}{\Delta} < \pi \frac{p_i}{p_i - 1}$$

for any subset $\{d_{i_1}, d_{i_2}, \ldots, d_{i_s}\}$ of $\mathcal{D}$. With N so chosen and using the definitions of δ and ε (equations (10) and (11)), we see that the expression in (9) is less than

$$MP\left\{\Sigma \frac{1}{d_i}\left(\prod_{i=1}^{t-1} \frac{p_i}{p_i - 1}\right) - \Sigma \frac{1}{[d_i, d_j]}\left(\prod_{i=1}^{t-1} \frac{p_i}{p_i - 1} - \varepsilon\right) + \ldots\right\}$$

$$= MP\, \pi \frac{p_i}{p_i - 1}\left\{\Sigma \frac{1}{d_i} - \Sigma \frac{1}{[d_i, d_j]} \cdots\right\} + MP\, \varepsilon\left\{\Sigma \frac{1}{[d_i, d_j]} + \Sigma \frac{1}{[d_i, d_j, d_k, d_\ell]} + \ldots\right\}$$

$$= (p_t - \delta) P\left\{\Sigma \frac{1}{d_i} - \Sigma \frac{1}{[d_i, d_j]} + \ldots\right\} + \frac{1}{2}\delta P\left\{\Sigma \frac{1}{d_i} - \Sigma \frac{1}{[d_i, d_j]} + \ldots\right\}$$

$$< p_t P\left\{\Sigma \frac{1}{d_i} - \Sigma \frac{1}{[d_i, d_j]} + \ldots\right\} . \tag{13}$$

This is an upper bound on the number of residue classes modulo $p_t P$ that can be covered by AP's in C. Expression (6) gave a lower bound on the number of residue classes modulo $p_t D$ that had to be covered by AP's in C. Since each residue class modulo $p_t D$ corresponds to P/D residue classes modulo $p_t P$ the number of residue classes mod $p_t P$ that must be covered by C is at least

$$\frac{P}{D} p_t D \left\{ \sum \frac{1}{d_i} - \sum \frac{1}{[d_i, d_j]} + \ldots \right\} \qquad (14)$$

Comparing (13) and (14) we see that the number of residue classes mod $p_t P$ that can be covered by C is less than the number that need to be covered. Thus it is not possible to form an ECS(M) not satisfying (2) and we are done. □

We now use theorem 4.12 to obtain some results about ECS(M)'s. For the most part similar results for naturally exact covering systems were obtained by Burshtein ([3]) who derived his results from his theorem 2.7 which is analogous to our theorem 4.12.

Corollary 4.13 The greatest prime p_t dividing the modulus of any AP in an ECS(M) is at most equal to the greatest prime p^* satisfying

$$M \prod_{p<p^*} \frac{p}{p-1} \geq p^* ,$$

where the product is over primes less than p^*.

Proof: Immediate from theorem 4.12. □

Remark 4.14 It is easily checked that

$$\frac{1}{p^*} \prod_{p<p^*} \frac{p}{p-1}$$

is strictly decreasing for $p^* \geqslant 3$, so p^* in the corollary is well defined. When $p^* = 2$ the expression equals $\frac{1}{2}$ and when $p^* = 3$ it equals 3/5, so it is always less than 1.

We now give an alternative proof of theorem 4.3.

Corollary 4.15 (= Theorem 4.3) The only ECS(1) is $\{<0,1>\}$.

Proof: If there did exist an ECS(1) with $P(A) \neq 1$ we would have a set of primes $p_1 < \ldots < p_t$ such that

$$p_t \leqslant \prod_{i=1}^{t-1} \frac{p_i}{p_i - 1} .$$

This would imply

$$1 \leqslant \frac{1}{p_t} \prod_{p<p_t} \frac{p}{p-1}$$

which is impossible by remark 4.14. □

The next corollary answers question I at the beginning of the chapter.

Corollary 4.16 For each positive integer M there exists a number B(M) such that in any ECS(M) the least modulus is less than B(M).

Proof: Let p^* be as in the statement of corollary 4.13, and let

$$\mathcal{D} = \{1 = \delta_1 < \delta_2 < \dots\}$$

be the set of integers all of whose prime factors are at most p^*. Then

$$M \sum_{i=1}^{\infty} \frac{1}{\delta_i} = M \prod_{p \leq p^*} \left(1 + \frac{1}{p} + \frac{1}{p^2} + \dots\right)$$

$$= M \prod_{p \leq p^*} \frac{p}{p-1}$$

and this is finite. There therefore exists an integer k such that k is the least integer for which

$$M \sum_{i=k}^{\infty} \frac{1}{\delta_i} < 1. \tag{15}$$

Now suppose an ECS(M) existed with each modulus $\geq \delta_k$. Since each such modulus must belong to $\mathcal{D}$ and each occurs in at most M AP's in the ECS(M), the sum of the reciprocals of these moduli is less than

$$M \sum_{i=k}^{\infty} \frac{1}{\delta_i}.$$

But according to theorem 4.1 the sum of the reciprocals equals 1 which contradicts (15). The statement of the corollary follows a setting $B(M) = \delta_k$. □

For the next corollary we need two more definitions.

Definition 4.17 We say that ECS(M)'s are *disjoint* if in the sequence $\wedge$ containing all their moduli each modulus occurs at most M times.

Definition 4.18 The maximal number of disjoint ECS(M)'s is denoted D(M).

Corollary 4.19 Let M be at least 2 and let p(M) be the least prime for which

$$M \prod_{p \leqslant p(M)} \frac{p}{p-1} < p(M). \tag{16}$$

Then

$$D(M) \leqslant p(M) - 2.$$

Proof: Suppose we have D(M) disjoint ECS(M)'s and that the moduli occurring in these ECS(M)'s are $\delta_1, \delta_2, \ldots, \delta_t$. By theorem 4.1 we have

$$\sum_{i=1}^{t} \frac{1}{\delta_i} = D(M)$$

and, as in the proof of corollary 4.16 we must have

$$\sum_{i=1}^{t} \frac{1}{\delta_i} < M \prod_{p<p(M)} \frac{p}{p-1}.$$

An easy rearrangement of (16) shows that the right hand side here is less than p(M) - 1. Thus

$$D(M) < p(M) - 1.$$

Since D(M) is an integer this implies our result. □

Corollary 4.20 If $p_1 < p_2 < \ldots < p_t$ are the distinct prime divisors of the moduli occurring in an ECS(M) then

$$p_1 \leqslant M.$$

The result is best possible since the set of residue classes modulo p is an ECS(p) for any prime p.

Proof: We suppose $p_1 > M$ and derive a contradiction.

First suppose $t = 1$ and p_1^{α} is the highest power of p_1 that divides any modulus in the ECS(M). Then for each positive i not exceeding α there are at most M residue classes mod p_1^{i}, and each of these covers $p_1^{\alpha-i}$ residue classes modulo p_1^{α}. Thus, since $M < p_1$, the total number of residue classes modulo p_1^{α} that are covered is at most

$$M(p_1^{\alpha-1} + p_1^{\alpha-2} + \ldots + 1) \leqslant (p_1-1)\frac{p_1^{\alpha}-1}{p_1-1} < p_1^{\alpha},$$

which is impossible for an exact covering system. Thus the case $t = 1$ cannot occur.

We may therefore assume t is greater than 1. We will show that

$$M < p_t \prod_{i=1}^{t-1} \frac{p_i-1}{p_i} \tag{17}$$

for any $t \geqslant 2$, and any set of primes

$$M < p_1 < \ldots < p_t .$$

We use induction on t. When $t = 2$ it is easy to check that (17) holds by using the inequalities $p_1 \geq M+1$, $p_2 \geq p_1 + 1$.

Now assume (17) holds when $t = t_0$. We show it also holds for $t = t_0 + 1$. We have

$$p_{t_0+1} \prod_{i=1}^{t_0} \frac{p_i - 1}{p_i} = p_{t_0+1} \frac{p_{t_0} - 1}{p_{t_0}^2} \left(p_{t_0} \prod_{i=1}^{t_0-1} \frac{p_i - 1}{p_i} \right)$$

$$\geq \frac{(p_{t_0} + 2)(p_{t_0} - 1)}{p_{t_0}^2} p_{t_0} \prod_{i=1}^{t_0-1} \frac{p_i - 1}{p_i}$$

$$> M,$$

by the induction hypothesis. Thus (17) holds for all t by induction whenever p_1 exceeds M. Rearranging (17) gives

$$M \prod_{i=1}^{t-1} \frac{p_i}{p_i - 1} < p_t$$

which contradicts theorem 4.12 when $p_1, p_2, \ldots, p_t$ are the prime divisors of the moduli of an ECS(M). This establishes the inequality in the corollary. □

We now rephrase this result using the following definition.

Definition 4.21 For a given prime p let

$$e(p) = \min\{M: \exists \text{ an ECS(M) in which no modulus is divisible by a prime less than } p\}.$$

Corollary 4.20' For all p

$$e(p) = p.$$

To compare this result with problems about general covering systems we make the following definitions.

Definition 4.22 An RCS(M) is a covering system, not necessarily exact, in which each modulus occurs at most M times.

Definition 4.23 For a given prime p let

$$r(p) = \min\{M: \exists \text{ an RCS}(M) \text{ in which no modulus is divisible by a prime less than } p\}.$$

It has been conjectured by Erdös [8] that $r(p)$ equals 1 for all p. In [7] he showed that $r(2) = 1$ but little progress has been made towards settling the conjecture for higher values of p. It may therefore be prudent to set oneself the more modest aim of finding a strong upper bound on $r(p)$ as a function of p. We end this chapter with a rather crude bound.

Theorem 4.24 For all p

$$r(p) \leqslant p - 1.$$

Proof: We construct an RCS(p-1) in which p is the smallest prime factor of any modulus. Let q be the least prime exceeding p. By Bertrand's postulate we have

$$3(p-1) \geqslant q. \tag{18}$$

We claim the following collection of AP's is the required RCS(p-1).

$\langle 1,p\rangle$, $\langle 2,p\rangle,\ldots,\langle p-1,p\rangle$

$\langle p,p^2\rangle$, $\langle 2p,p^2\rangle,\ldots,\langle (p-1)p,p^2\rangle$

$\langle 0,q\rangle$, $\langle 1,q\rangle,\ldots,\langle p-2,q\rangle$

$\langle p-1,q\rangle \cap \langle 0,p\rangle, \langle p,q\rangle \cap \langle 0,p\rangle,\ldots,\langle 2p-3,q\rangle \cap \langle 0,p\rangle$

$\langle 2p-2,q\rangle \cap \langle 0,p^2\rangle$, $\langle 2p-1,q\rangle \cap \langle 0,p^2\rangle$ $,\ldots,\langle 3p-4,q\rangle \cap \langle 0,p^2\rangle$.

To see this note that the first two rows cover all integers not congruent to 0 modulo p^2 and that AP's in the last three rows together cover all AP's of the form $\langle i,q\rangle \cap \langle 0,p^2\rangle$ with i going from 0 to $3p-4$. By (18) i therefore runs through a complete residue system modulo q, and so the system covers the integers. It is then clearly an RCS(p-1).

□

CHAPTER 5

THE CRITTENDEN AND VANDEN EYNDEN CONJECTURE : CHARACTERISATION OF A COUNTER EXAMPLE

For most of the remainder of this thesis we will consider the following conjecture, due to R.B. Crittenden and C.L. Vanden Eynden [5]. In the final part of Chapter 7 we will introduce and examine a new conjecture which is akin to this one.

Conjecture 5.1 Let n and k be positive integers with $n \geq k$. If A is a collection of n AP's, each having modulus at least k and such that

$$Z(A) \supseteq [1, k2^{n-k+1}]$$

then

$$Z(A) = \mathbb{Z} .$$

This conjecture is equivalent in the cases $k = 1$ and $k = 2$ since for either value we have

$$k2^{n-k+1} = 2^n .$$

The following observation has been made by Crittenden and Vanden Eynden [5].

Theorem 5.2 The conjecture does not hold if $k2^{n-k+1}$ is replaced by a smaller integer.

Proof: Let

$$A = \{\langle i,k\rangle : i = 1,\ldots,k-1\} \cup \{\langle 2^{i-1}k, 2^i k\rangle : i = 1,\ldots,n-k+1\}.$$

It is easily seen that

$$Z(A) \supset [1, k2^{n-k+1} - 1]$$

and

$$Z(A) \neq \mathbb{Z}.$$ □

The history of the conjecture begins with the following conjecture by Stein [23].

Conjecture 5.3 If A is a collection of n pairwise disjoint AP's with distinct moduli, none of which is $\langle 0,1\rangle$, then there is at least one integer m, $1 \leqslant m \leqslant 2^n$, which does not belong to $Z(A)$.

In this conjecture it is not necessary to state that

$$Z(A) \neq \mathbb{Z}$$

since equality here would mean we had a non-trivial ECS(1). This is impossible by theorem 4.3.

Erdös [9] showed that this conjecture would hold if 2^n was replaced with $n2^n$. He then made a stronger conjecture corresponding to the $k = 1$ (or 2) case of conjecture 5.1. This was proven by Crittenden and Vanden Eynden in 1970 [4]. We state it as a theorem.

Theorem 5.4 If A is a collection of n AP's such that

$$Z(A) \supseteq [1, 2^n]$$

then

$$Z(A) = \mathbb{Z} .$$

An announcement of a proof was also made by J. Selfridge [21] at a meeting of the American Mathematical Society, though apparently his proof was never published.

Erdös, in a private communication, suggested to Crittenden and Vanden Eynden that they consider collections of AP's having modulus at least 3 which covered an initial interval of the integers without covering them all. Crittenden and Vanden Eynden replaced 3 with an arbitary positive integer k and made conjecture 5.1. This first appeared in the American Mathematical Monthly [5] and has since been published by Guy [11] and Porubsky [19].

Remark 5.5 It is easy to see that the intervals $[1,k2^{n-k+1}]$ and $[1,2^n]$ appearing in the statements of conjecture 5.1 and theorem 5.4 respectively could be replaced by any intervals of the form

$$[b+1,\ b+k2^{n-k+1}] \quad \text{and} \quad [b+1,\ b+2^n]$$

respectively, without altering the truth of either statement. This observation allows us to simplify some of our proofs.

In this thesis we will not prove that conjecture 5.1 holds for all values of n and k but instead make the following contributions to such a proof.

(a) Conjecture 5.1 holds for $k = 3$ and all $n \geqslant 3$.

(b) If the conjecture fails for some k then it fails for that k and for some n less than

$$3(\theta(k)/\log 2+k) - 2\pi(k) + 18\log_2 k + \lceil \log_2 k \rceil + (3\log_2 3-4)\lceil \log_3 k \rceil$$

where $\theta(k)$ and $\pi(k)$ have their usual meanings (see notation 1.1).

These results will not be proven until Chapter 7. In this chapter we obtain a number of properties which a minimal counterexample (defined below) to the conjecture must possess. These will give us a sufficiently precise characterisation of such a counterexample to apply a sieve technique. The sieve itself is the subject of the next chapter, and is applied in Chapter 7. Like most sieve results this one only gives the required bound when some parameter, in our case n, is sufficiently large. Thus to prove the conjecture for some value of k it is necessary to check the low values of n one by one. We do this for $k = 3$ in Chapter 7.

We now define a minimal counterexample.

Definition 5.6 For a given positive integer k we define a *minimal counterexample* for this k as a collection A of n AP's, each with modulus at least k, and such that

$$Z(A) \supseteq [1,k2^{n-k+1}]$$

and

$$Z(A) \neq \mathbb{Z}$$

and further such that (a) n is the least integer for which such an A exists and (b) in any other collection of n AP's having these properties the sum of the moduli of the AP's is at least equal to the sum of the moduli of the AP's in A.

In obtaining necessary conditions for A to be a minimal counterexample we will often use proof by contradiction, showing that if 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 decreased. In the proofs it will sometimes be convenient to assume that 0 is not covered by A. We now show that this can be done without loss of generality.

Theorem 5.7 If there exists a minimal counterexample for a given value of k then there exists a minimal counterexample for that k which does not cover 0 and which has the same cardinality and the same moduli.

Proof: Let A^* be a minimal counterexample. Since $Z(A^*)$ does not equal $\mathbb{Z}$ we know there exists an integer, x_0 say, which does not belong to any AP in A^*. This will also be so for any x satisfying

$$x \equiv x_0 \pmod{P(A^*)}.$$

Thus there are non-positive integers which do not belong to $Z(A^*)$. Let y be the greatest of these. Now let

$$A = \{\langle a-y,d\rangle : \langle a,d\rangle \in A^*\}$$

and we have

$$Z(A) \supseteq [1,k2^{n-k+1}]$$

$$Z(A) \not\supseteq \{0\}.$$

□

Our first necessary condition for a minimal counter-example is the following:

Theorem 5.8 If A is a minimal counterexample then

$$|A| > k.$$

Proof: We must show the conjecture holds when $n = k$. Suppose we have a collection

$$A = \{\langle a_i, d_i \rangle : i = 1,\ldots,k\}$$

with

$$d_i \geqslant k \quad \text{for} \quad i = 1,\ldots,k$$

$$Z(A) \supseteq [1,2k].$$

Each of the integers $1,2,\ldots,k$ must be included in a different member of A (otherwise the AP would have common difference less than k) so A has the form

$$A = \{\langle i, d_i \rangle : i = 1,\ldots,k\}.$$

The integer $k+1$ must be covered by one of these. The only one that can do this is $\langle 1, d_1 \rangle$ so we have $d_1 = k$. By considering $k + 2$ we then find $d_2 = k$ and so on so that

$$d_i = k \quad \text{for} \quad i = 1,\ldots,k.$$

But now we have $Z(A) = \mathbb{Z}$ as predicted by the conjecture.

□

The rest of this chapter will be concerned with constraints on the moduli of the AP's in a minimal counterexample. Our first is given in the following theorem.

Theorem 5.9 If A is a minimal counterexample which does not cover 0, and $\langle a,bc\rangle$ belongs to A with $b \geq k$, $c > 1$, then

(a) $Z(A) \supseteq \mathbb{Z} \setminus \langle 0,b\rangle$,

(b) $a \equiv 0 \pmod{b}$,

(c) $\langle a,bc\rangle \subseteq \langle 0,b\rangle$.

Proof: Write

$$A = A^* \cup \{\langle a,bc\rangle\}.$$

Now $\langle a,b\rangle \supset \langle a,bc\rangle$, so

$$Z(A^* \cup \{\langle a,b\rangle\}) \supseteq Z(A) \supseteq [1,k2^{n-k+1}].$$

This means that $A^* \cup \{\langle a,b\rangle\}$ is a counterexample to the conjecture, contradicting the minimality of A, unless

$$Z(A^* \cup \{\langle a,b\rangle\}) = \mathbb{Z}, \tag{1}$$

so we conclude that this is so. We assumed that A, and therefore A^*, do not cover 0, so 0 must belong to $\langle a,b\rangle$. That is,

$$a \equiv 0 \pmod{b}.$$

This is part (b) of the theorem. Part (a) then follows from (1), and part (c) from part (d) of theorem 2.1. □

Using this we prove

Corollary 5.10 Suppose A is a minimal counterexample that does not cover 0, and $\langle a,d\rangle$ is an element of A.

(a) If $2^{\alpha} \| d$ and $2^{\alpha} \geqslant k$ then

$$d = 2^{\alpha}.$$

(b) If p is an odd prime, $p^{\alpha+1} \| d$ and $p^{\alpha} \geqslant k$ then

$$d = p^{\alpha+1}.$$

Proof: (a) Suppose $d = 2^{\alpha}d_o$ where d_o is odd and greater than 1. Then by part (b) of theorem 5.9, with 2^{α} in the role of b and d_o in the role of c, we have

$$a \equiv 0 \pmod{2^{\alpha}}. \tag{2}$$

Since we also have $2^{\alpha-1}d_o > k$ we use part (b) again with $2^{\alpha-1}d_o$ in the role of b to give

$$a \equiv 0 \pmod{2^{\alpha-1}d_o}. \tag{3}$$

Together (2) and (3) imply

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

which implies A covers 0, a contradiction.

(b) Suppose $d = p^{\alpha+1}d_o$ where $d_o > 1$ and p is an odd prime which does not divide d_o. We again apply part (b)

of theorem 5.9 twice, first with $p^{\alpha+1}$ in the role of b and second with $p^{\alpha}d_o$ in that role, obtaining

$$a \equiv 0 \pmod{p^{\alpha+1}}$$

$$a \equiv 0 \pmod{p^{\alpha}d_o}.$$

This leads to a contradiction as in part (a). □

Note that theorem 5.9 does not enable us to forbid all AP's with modulus $p^{\alpha}d_o$ with $p^{\alpha} \geqslant k$ and $d_o > 1$. If d_o is a prime or prime power with

$$d_o p^{\alpha-1} < k$$

we cannot obtain a contradiction by arguing as in corollary 5.10.

The next five results do improve on corollary 5.10 in the special case of primes which are at least k.

Theorem 5.11 If A is a minimal counterexample and p a prime, then for all integers b we have

$$Z(A) \not\subseteq \mathbb{Z} \setminus \langle b,p \rangle.$$

Proof: Suppose otherwise so that $A \cup \{\langle b,p \rangle\}$ covers the integers and any regular subcovering of it must contain $\langle b,p \rangle$. By corollary 2.6 A therefore contains at least $p - 1$ AP's whose moduli are divisible by p and which are disjoint from $\langle b,p \rangle$.

We now reduce the collection

$$\{\langle a,d \rangle \in A : \langle a,d \rangle \cap \langle b,p \rangle \neq \phi\}$$

via $\langle b,p\rangle$, as in definition 2.7, to obtain a collection A^* with

$$|A^*| \leqslant n - p + 1. \tag{4}$$

Now A being a counterexample implies

$$Z(A) \supseteq [1,k2^{n-k+1}] \cap \langle b,p\rangle$$

$$= \{b + ip : i = 0,\ldots,[k2^{n-k+1}/p] - 1\}.$$

Here we have assumed, as we may, that $1 \leqslant b \leqslant p$. By part (d) of corollary 2.12 we then have

$$Z(A^*) \supseteq [0,[k2^{n-k+1}/p] - 1]. \tag{5}$$

Also, since

$$Z(A) \supseteq \mathbb{Z}\backslash\langle b,p\rangle,$$

$$Z(A) \neq \mathbb{Z}$$

we have

$$Z(A) \not\supseteq \langle b,p\rangle.$$

By part (a) of corollary 2.12 we therefore have

$$Z(A^*) \neq \mathbb{Z}.$$

By remark 5.5 with $b = -1$, theorem 5.4 and equation (5) we therefore 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

$$p \geqslant k \geqslant 2.$$

This contradiction proves the theorem. □

Corollary 5.12 Suppose A is a minimal counterexample and p is a prime at least k and $\langle a,pd \rangle$ belongs to A, then $d = 1$.

Proof: Suppose that $d \neq 1$. We may then form another minimal counterexample A^* as in theorem 5.7 which does not cover 0 and whose elements have the same moduli as the corresponding elements of A. Then by part (a) of theorem 5.9 we have

$$Z(A^*) \supseteq \mathbb{Z} \setminus \langle 0,p \rangle$$

which contradicts theorem 5.11. □

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 AP's with prime modulus.

Lemma 5.13 Any AP $\langle a,d\rangle$ is equal to the union of $\lceil k/d \rceil$ AP's each having modulus at least k.

Proof: It is easily seen that

$$\langle a,d\rangle = \bigcup_{i=1}^{\lceil k/d \rceil} \langle a + id, \lceil k/d \rceil d\rangle$$

and that

$$\lceil k/d \rceil d \geqslant k.$$

□

Theorem 5.14 If A is a minimal counterexample and $\langle a_o,d_o\rangle$ is an AP such that $d_o \geqslant 2$ and

$$z(A) \notin \langle a_o,d_o\rangle$$

then

$$\sum_{\substack{\langle a,d\rangle \in A,(d,d_o)>1 \\ a \equiv a_o \pmod{(d,d_o)}}} \frac{\lceil k(d,d_o) \rceil}{d} + \log_2 d_o > |\{\langle a,d\rangle \in A : (d,d_o)>1\}| \qquad (6)$$

Proof: We set

$$A_1 = \{\langle a,d\rangle \in A : (d,d_o) > 1,\ a \equiv a_o \pmod{(d,d_o)}\}$$

$$A_2 = \{\langle a,d\rangle \in A : (d,d_o) > 1,\ a \not\equiv a_o \pmod{(d,d_o)}\}$$

$$A_3 = \{\langle a,d\rangle \in A : (d,d_o) = 1\},$$

and

$$|A_i| = N_i \qquad (i = 1,2,3).$$

No AP in A_2 will intersect $\langle a_o,d_o\rangle$ so

$$Z(A_1 \cup A_3) \supseteq \langle a_o, d_o \rangle \cap [1, k2^{n-k+1}].$$

If we assume, as we may, that

$$1 \leqslant a_o \leqslant d_o$$

then this means

$$Z(A_1 \cup A_3) \supseteq \{a_o + id_o : i = 0, \ldots [(k2^{n-k+1} - a_o)/d_o]\}.$$

We now reduce A_1 and A_3 via $\langle a_o, d_o \rangle$ to A_1^* and A_3^* respectively so that, by part (d) of corollary 2.12,

$$Z(A_1^* \cup A_3^*) \supseteq [0, [(k2^{n-k+1} - a_o)/d_o]]$$

$$\supseteq [0, [k2^{n-k+1}/d_o] - 1].$$

From this we see that

$$Z(\{\langle a+1, d \rangle : \langle a, d \rangle \in A_1^* \cup A_3^*\}) \supseteq [1, [k2^{n-k+1}/d_o]]. \qquad (7)$$

By theorem 2.10 and our assumption that $Z(A)$ does not include $\langle a_o, d_o \rangle$ the collection in (7) does not cover the integers. It thus has some of the properties of a counter-example to conjecture 5.1. However the reduction of an AP $\langle a, d \rangle$ via $\langle a_o d_o \rangle$ has modulus

$$d/(d, d_o)$$

and in the case of those AP's in A_1^* this may be less than k. To overcome this difficulty we use lemma 5.13 to replace each AP that appears in the collection in (7) and originated in A_1 with

$$\lceil k(d,d_o)/d \rceil$$

AP's each having modulus at least k. We combine this collection with

$$\{\langle a+1,d\rangle : \langle a,d\rangle \in A^*_3\}$$

to form a new collection $\mathcal{B}$ say. $Z(\mathcal{B})$ is then identical to the left hand side of (7), each modulus appearing in it is at least k and

$$|\mathcal{B}| = \sum_{\langle a,d\rangle \in A_1} \lceil k(d,d_o)/d \rceil + N_3$$

$$= N, \quad \text{say.} \tag{8}$$

By (7) and the remarks following it we also have

$$Z(\mathcal{B}) \supseteq [1,[k2^{n-k+1}/d_o]],$$

$$Z(\mathcal{B}) \neq \mathbb{Z}.$$

Now the sum appearing in (8) is the sum that appeared in (6). If it is at least $N_1 + N_2$ we have already established inequality (6) 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

$$|\mathcal{B}| < N_1 + N_2 + N_3 = n.$$

Since A is a minimal counterexample we therefore have

$$[k2^{n-k+1}/d_o] < k2^{N-k+1}.$$

This leads to

$$N > n - \log_2 d_o.$$

On substituting for N and n and recalling the definitions of A_1 and A_2 we obtain the required inequality.

□

Corollary 5.15 If A is a minimal counterexample and p is a prime at least k then the number of AP's in A having modulus p is less than $\log_2 p$.

Proof: By corollary 5.12 the only AP's in A having modulus divisible by p have modulus equal to p. We can therefore choose a residue class modulo p, $\langle a_o, p\rangle$ say, which intersects no AP in A with modulus divisible by p.

We now use $\langle a_o, p\rangle$ in the role of $\langle a_o, d_o\rangle$ in theorem 5.14. By the preceding remark we see that the sum that appears in the statement of that theorem is empty. We then have

$$\log_2 p > |\{\langle a,d\rangle \in A : (d,p) > 1\}|$$

$$= |\{\langle a,d\rangle \in A : d = p\}|.$$

□

We have shown that if p is a prime at least k then the only moduli divisible by p which can occur in a minimal counterexample must equal p and that the number of AP's with modulus p is less than $\log_2 p$. The final results of this chapter concern those moduli which are divisible by primes less than k.

Theorem 5.16 If A is a minimal counterexample which does not cover 0, p is a prime less than k and A includes a subcollection

$$\{\langle ip^{\alpha-1}, p^{\alpha}\rangle : i = 1,\ldots,p-1\}$$

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

$$\alpha \geqslant \lceil \log k/\log p \rceil. \tag{9}$$

Suppose we have strict inequality in (9) and write

$$A = A_1 \cup A_2 \cup A_3$$

where

$$A_1 = \{\langle a,d\rangle \in A : p^{\alpha+1} | d\}$$

$$A_2 = \{\langle a,d\rangle \in A : p^{\alpha} \parallel d\}$$

$$A_3 = \{\langle a,d\rangle \in A : p^{\alpha} \nmid d\}.$$

Now by hypothesis,

$$|A_2| \geqslant p - 1$$

and by our supposition

$$p^{\alpha-1} \geqslant k.$$

Corollary 5.10 and theorem 5.9 then imply that any AP $\langle a,d\rangle$ in A_2 has the form

$$\langle ip^{\alpha-1}, p^{\alpha}\rangle$$

and that

$$Z(A) \supseteq \mathbb{Z} \setminus \langle 0, p^{\alpha-1}\rangle .$$

Since A does not cover 0 no member of A_2 has the form $\langle 0,p^{\alpha}\rangle$ so

$$Z(A_2) \subseteq \langle 0,p^{\alpha-1}\rangle \setminus \langle 0,p^{\alpha}\rangle .$$

Similarly we have

$$Z(A_1) \subseteq \langle 0,p^{\alpha}\rangle .$$

These last three inclusions imply

$$Z(A_3 \cup \langle 0,p^{\alpha-1}\rangle) \supseteq \mathbb{Z} .$$

We now use the transformation T_p introduced in definition 2.13. By theorem 2.14 the above display gives

$$Z(T_p(A_3) \cup T_p(\langle 0,p^{\alpha-1}\rangle)) \supseteq \mathbb{Z} .$$

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

$$Z(T_p(A_3)) \supseteq \mathbb{Z} \setminus \langle 0,p^{\alpha-1}\rangle . \tag{10}$$

We now turn our attention to the collection A_1. If $\langle a,d\rangle$ is an element of this then by its definition and

corollary 5.9(b) both a and d are divisible by p. We form another collection

$$A^*_1 = \{\langle a/p, d/p\rangle : \langle a,d\rangle \in A_1\}$$

and note that each modulus appearing in A^*_1 is at least p^α which is at least k.

Since we have shown that $Z(A_2)$ is disjoint from $\langle 0, p^\alpha\rangle$ we have

$$Z(A_1 \cup A_3) \supseteq \langle 0, p^\alpha\rangle \cap [1, k2^{n-k+1}]$$

$$= \{ip^\alpha : i = 1, \ldots, [k2^{n-k+1}/p^\alpha]\} .$$

It is easy to check that ip^α belongs to an AP in A_1 if and only if $ip^{\alpha-1}$ belongs to the corresponding AP in A^*_1. Also, by theorem 2.15 ip^α belongs to an AP in A_3 if and only if $ip^{\alpha-1}$ belongs to the equivalent AP in $T_p(A_3)$. Thus

$$Z(A^*_1 \cup T_p(A_3)) \supseteq \{ip^{\alpha-1} : i = 1, \ldots, [k2^{n-k+1}/p^\alpha]\}$$

$$Z(A^*_1 \cup T_p(A_3)) \not\supseteq \{0\}.$$

Since by (10) the collection $A^*_1 \cup T_p(A_3)$ covers all integers which are not divisible by $p^{\alpha-1}$, the least integer not covered by the collection is at least

$$[k2^{n-k+1}/p^\alpha]p^{\alpha-1} + p^{\alpha-1}$$

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

$$\geqslant [k2^{n-k+1}/p].$$

We therefore have

$$Z(A^*_1 \cup T_p(A_3)) \supseteq [1, [k2^{n-k+1}/p]]$$

$$Z(A^*_1 \cup T_p(A_3)) \neq \mathbb{Z}$$

$$|A^*_1 \cup T_p(A_3)| \leqslant n - p + 1,$$

and each AP in the collection has modulus at least k. Since A was assumed minimal we must have

$$[k2^{n-k+1}/p] < k2^{n-p-k+2}$$

which leads to

$$2^p < 2p$$

which is impossible for $p \geqslant 2$. This contradiction proves our theorem. □

Corollary 5.17 Suppose that A is a minimal counter-example that does not cover 0.

(a) The highest power of 2 dividing $P(A)$ is at most $2^{\lceil \log_2 k \rceil}$.

(b) If p is an odd prime less than k then the highest power of p dividing $P(A)$ is at most $p^{\lceil \log_p k \rceil + 1}$.

Proof: (a) Let 2^α be the highest power of 2 dividing $P(A)$. Then A contains an AP of the form $\langle a, 2^\alpha d\rangle$. If $2^{\alpha-1}$ is less than k we are done, and if $2^{\alpha-1}$ is at least k we have, by theorem 5.9 and corollary 5.10

$$\langle a, 2^\alpha d\rangle = \langle 2^{\alpha-1}, 2^\alpha\rangle.$$

By theorem 5.16 we then have $\alpha = \lceil \log k/\log 2 \rceil$ as required.

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

$$\alpha > \lceil \log k/\log p \rceil. \tag{11}$$

Then A contains an AP of the form $\langle a,p^{\alpha}d\rangle$. By theorem 5.9 we have

$$Z(A) \supseteq \mathbb{Z} \setminus \langle 0,p^{\alpha}\rangle.$$

In particular $Z(A)$ covers $\langle ip^{\alpha-1},p^{\alpha}\rangle$ for $i = 1,\ldots,p-1$. Since $Z(A)$ does not cover $\langle 0,p^{\alpha}\rangle$ we may apply corollary 3.3 and find that A contains $p - 1$ AP's of the form $\langle a_i,p^{\alpha}d_i\rangle$ with

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

By theorem 5.10 each d_i equals 1, so these AP's are precisely

$$\{\langle ip^{\alpha-1},p^{\alpha}\rangle : i = 1,\ldots,p-1\}.$$

But now theorem 5.16 says that α equals $\lceil \log k/\log p \rceil$, contradicting (11).

□

CHAPTER 6

A SIEVE FOR THE CRITTENDEN AND VANDEN EYNDEN CONJECTURE

In the last chapter we obtained some conditions which a minimal counterexample to conjecture 5.1 must possess. Our aim is to show that a collection of n AP's satisfying these conditions cannot cover the first $k2^{n-k+1}$ positive integers. In this chapter we will be concerned with AP's having prime modulus $\geqslant k$, and will derive an upper bound on the length of an interval that can be covered by n such AP's. In the next chapter we will apply this result to the conjecture. We begin with some notation.

Notation 6.1 Throughout this chapter A will be a collection of AP's, each having prime modulus, and k a positive integer $\geqslant 3$. For each prime p we put

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

The collection A will satisfy the following conditions.

$$|A| = n, \tag{1}$$

$$c(p) = 0 \quad \text{if} \quad p < k, \tag{2}$$

$$c(p) \leqslant [\log_2 p] \quad \text{otherwise.} \tag{3}$$

Our first theorem in this chapter gives some lower bounds on the number of positive integers $\leqslant N$ which do

not belong to $Z(A)$. It is essentially the same as Lemma 2 of Crittenden and Vanden Eynden [4].

Theorem 6.2 Let A be a collection of n AP's each having prime modulus. Let $p_1, p_2, \ldots, p_t$ be the moduli occurring in A and for each i in the interval $[1,t]$ let

$$c_i = c(p_i)$$

be the number of AP's in A with modulus p_i. Then we have:

(a) If s is an integer such that $1 \leqslant s \leqslant t$ and N is a positive integer then

$$|\{m : 1 \leqslant m \leqslant N, \quad m \notin Z(A)\}|$$

$$> N\Big(1 - \sum_{i=s}^{t} c_i/p_i\Big) \prod_{i=1}^{s-1}(1 - c_i/p_i) - \Big(1 + \sum_{i=s}^{t} c_i\Big)\prod_{i=1}^{s-1}(1+c_i).$$

(b) $$|\{m : 1 \leqslant m \leqslant N, \quad m \notin Z(A)\}|$$

$$\geqslant N - c_1\left(\left[\frac{N}{p_1}\right] + 1\right) - \sum_{i=2}^{t} c_i\left(\left[\frac{N}{p_i}\right] - c_1\left[\frac{N}{p_1 p_i}\right] + 1\right)$$

(c) $$|\{m : 1 \leqslant m \leqslant N, \quad m \notin Z(A)\}|$$

$$\geqslant N - \sum_{i=1}^{t} c_i\left(\left[\frac{N}{p_i}\right] + 1\right) + c_1 c_2\left[\frac{N}{p_1 p_2}\right] + \sum_{i=3}^{t} c_i\Big(c_1\left[\frac{N}{p_1 p_i}\right]$$

$$+ c_2\left[\frac{N}{p_2 p_i}\right] - c_1 c_2\left(\left[\frac{N}{p_1 p_2 p_i}\right] + 1\right)\Big)$$

Proof: We shall use Σ' to denote a sum in which at most one of the subscripts is $\geqslant s$ and all relevant subscripts are covered. We note that with this notation for any $x_1, x_2, \ldots, x_t$

$$1 + \Sigma' x_i + \Sigma' x_i x_j + \ldots + \Sigma' x_{i_1} x_{i_2} \ldots x_{i_s}$$

$$= (1 + \sum_{i=s}^{t} x_i) \prod_{i=1}^{s-1} (1 + x_i). \tag{4}$$

For $i = 1,2,\ldots,t$ we let S_i be the union of those AP's in A which have modulus p_i. It follows from the Chinese Remainder Theorem that each set of $p_{i_1} p_{i_2} \ldots p_{i_\ell}$ consecutive integers contains exactly $c_{i_1} c_{i_2} \ldots c_{i_\ell}$ elements of $S_{i_1} \cap S_{i_2} \ldots \cap S_{i_\ell}$ and hence that

$$|S_{i_1} \cap S_{i_2} \cap \ldots \cap S_{i_\ell} \cap [1,N]|$$

$$= \prod_{j=1}^{\ell} c_{i_j} \left[N / \prod_{j=1}^{\ell} p_{i_j} \right] + E \prod_{j=1}^{\ell} c_{i_j} \tag{5}$$

where E satisfies

$$0 \leqslant E \leqslant 1.$$

It follows that

$$|S_{i_1} \cap S_{i_2} \cap \ldots \cap S_{i_\ell} \cap [1,N]|$$

$$= N \prod_{j=1}^{\ell} c_{i_j} / p_{i_j} + E' \prod_{j=1}^{\ell} c_{i_j} \tag{6}$$

where E' satisfies

$$-1 < E' < 1.$$

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

$$\chi_{\mathbb{Z}\setminus Z(A)} = \prod_{i=s}^{t}(1-\chi_{S_i}) \prod_{i=1}^{s-1}(1-\chi_{S_i})$$

$$\geqslant (1 - \sum_{i=s}^{t} \chi_{S_i}) \prod_{i=1}^{s-1}(1-\chi_{S_i}).$$

Using identity (4) with $-\chi_{S_i}$ in the role of x_i we obtain

$$\chi_{\mathbb{Z}\setminus Z(A)} \geqslant 1 - \sum_{i}{}' \chi_{S_i} + \sum_{i,j}{}' \chi_{S_i}\chi_{S_j} - \ldots$$

Using the fact that for any sets A and B

$$\chi_{A \cap B} = \chi_A \chi_B$$

we obtain

$$|\{m : 1 \leqslant m \leqslant N, \quad m \notin Z(A)\}|$$

$$= \sum_{m=1}^{t} \chi_{\mathbb{Z}\setminus Z(A)}(m)$$

$$\geqslant N - \sum_{i}{}' |S_i \cap [1,N]| + \sum_{i,j}{}' |S_i \cap S_j \cap [1,N]| - \ldots \qquad (7)$$

Using equation (6) we see that the right hand side of (7) is greater than

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

We now collect those terms involving N and those not involving N and apply identity (4) to each collection of terms and obtain part (a) of the theorem.

To obtain part (b) we set $s = 2$. Using (7) and inequality (5) we obtain

$$|\{m : 1 \leq m \leq N,\ m \notin Z(A)\}|$$

$$N - \sum_{i=1}^{t} (c_i[N/p_i] + c_i) + \sum_{i=2}^{t} c_1 c_i [N/p_1 p_i],$$

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 $s = 3$.

□

Parts (b) and (c) of this theorem will be used in Chapter 7. We use part (a) to derive a corollary, but first we must introduce some notation.

Notation 6.3 For any collection A of AP's we set

$$M(A) = \max\{N : Z(A) \supseteq [1,N]\}.$$

If $Z(A)$ does not include 1 we set $M(A) = 0$.

Corollary 6.4 Let A be a collection of AP's satisfying the conditions of notation 6.1, and p_o a prime dividing $P(A)$ such that

$$1 - \sum_{p \geq p_o} c(p)/p > 0.$$

(This will hold for sufficiently large p_o since the number of non-zero $c(p)$'s is finite.) Then

$$M(A) < \frac{1 + \sum_{p \geqslant p_o} c(p)}{1 - \sum_{p \geqslant p_o} c(p)/p} \prod_{p<p_o} \frac{1 + c(p)}{1 - c(p)/p}. \qquad (8)$$

Proof: By the definition of $M(A)$ we have

$$|\{m : 1 \leqslant m \leqslant M(A), \quad m \notin Z(A)\}| = 0.$$

Thus we may use part (a) of the theorem with 0 replacing the left hand side of the inequality and $M(A)$ replacing N on the right and p_o in the role of p_s. An easy rearrangement then gives (8). □

The rest of this chapter is devoted to getting upper bounds for $M(A)$. This requires getting an upper bound for the right hand side of (8) which is independent of the values of the variables $c(p)$. To do this we need some more notation.

Notation 6.5 We set:

p is an odd prime,

p' is the prime preceding p,

x is a positive real number,

$$A(x) = \prod_{p<x} \frac{p}{p-1},$$

$$W(p) = p' - [\log_2 p'],$$

$$V(x,p) = \frac{1 + x}{1 - x/p} 2^{-x},$$

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

$$r - 1 + \sum_{k \leqslant p < r} [\log_2 p] \geqslant n.$$

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

We now obtain some bounds for these functions.

Lemma 6.6 For $p \geqslant 7$ we have

$$p - 4 \geqslant W(p) > 2.$$

Proof: For such p,

$$[\log_2 p'] \geqslant 2$$

and so

$$W(p) \leqslant p' - 2 \leqslant p - 4.$$

Also, for $p' \geqslant 5$ we have

$$\log_2 p' < p'/2$$

and so

$$W(p) > p'/2 > 2.$$

□

Theorem 6.7 For fixed $p \geqslant 7$ the function $V(x,p)$, defined in notation 6.5, 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

$$\frac{f'(x)}{f(x)} = \frac{p+1}{(1+x)(p-x)} - \log 2$$

$$\leqslant \frac{p+1}{2(p-1)} - \log 2,$$

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

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

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

Corollary 6.8 If m is an integer satisfying

$$0 \leqslant m \leqslant [\log_2 p]$$

then

$$V(m,p) \leqslant p/(p-1) \tag{9}$$

Proof: We have

$$1 \leqslant [\log_2 p]$$

for all primes and

$$[\log_2 p] \begin{cases} = 1 & \text{if } p = 2 \text{ or } 3 \\ = 2 & \text{if } p = 5 \\ \leqslant p-2 & \text{if } p > 5. \end{cases}$$

We have

$$V(0,p) = 1, \quad V(1,p) = p/(p-1), \quad V(2,5) = 5/4.$$

So (9) holds for $p = 2,3,5$. If $p \geqslant 7$ we use theorem 6.7 which says that $V(m,p)$ attains its maximum value in the interval $[1,p-2]$ when $m = 1$. Thus (9) holds for all primes. □

Corollary 6.9 The function $A(p)V(W(p),p)$ is strictly decreasing for $p \geqslant 5$.

Proof: It is easily checked that

$$A(7)V(W(7),7) \leqslant A(5)V(W(5),5)$$

using $W(5) = 2$, $W(7) = 3$. We therefore assume $p \geqslant 7$ and let p^+ be the prime immediately succeeding p. Using lemma 6.6 and the definition of W we then have

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

Applying theorem 6.7 we then have

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

Using the bounds on $W(p)$ in lemma 6.6 this is at most

$$\begin{aligned} & \frac{1}{2}\left(1 + \frac{1}{3}\right)\left(1 + \frac{1}{p-3}\right) V(W(p),p) \\ =\ & \frac{2}{3}\left(\frac{p-2}{p-3}\right)V(W(p),p) \end{aligned}$$

$$< \frac{p-1}{p} V(W(p),p),$$

for $p \geqslant 7$. Since

$$A(p^+) = \frac{p}{p-1} A(p)$$

this establishes the corollary. □

Lemma 6.10 If m is an integer, $m \geqslant 2$, we have

$$A(m) < 2 \log m.$$

Proof: By direct calculation we find the inequality holds for $m \leqslant 18$. For higher values we use the following known result (Rosser and Schoenf eld [20], theorem 8, corollary 1),

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

This holds for all real m exceeding 1. If $m \geqslant 19$ then the right hand side is less than

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

$$< 2 \log m.$$

□

Lemma 6.11 With $r = r(k,n)$ as defined in notation 6.5, and with $r' = r'(k,n)$ being the prime preceding $r(k,n)$ we have for $k \geqslant 3$ and $n \geqslant 10$:

(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

$$r \leqslant 2n/5$$

the inequality defining $r(3,n)$,

$$r - 1 + \sum_{3 \leqslant p < r} [\log_2 p] \geqslant n \tag{10}$$

does not hold.

We note that

$$\sum_{3 \leqslant p < r} [\log_2 p] < \sum_{p<r} \log_2 p - 1,$$

$$\leqslant \theta(r)/\log 2 - 1,$$

where $\theta(r)$ has its usual meaning (see notation 1.1). Now Rosser and Schoenfield [20], theorem 9 states that for $x > 1$

$$\theta(x) < 1.01624x.$$

Applying this we find that for $r \leqslant 2n/5$

$$r - 1 + \sum_{3 \leqslant p < r} [\log_2 p] < r + (1.017/\log 2)r$$

$$< n$$

contradicting (10).

(b) This may be checked for values of $9 < m < 57$. If $n \geqslant 57$ we have $r(3,n) \geqslant 31$. Nagura [17] has shown that for $p' \geqslant 29$

$$p' > 5p/6.$$

Applying this and part (a) of the lemma gives the result.

(c) Let $s(n)$ be the least prime satisfying

$$s(n) - 1 \geqslant n.$$

Clearly $s(n) \geqslant r(k,n)$ for all k so it is sufficient to show

$$s(n) \leqslant 2n,$$

and this follows from Bertrand's postulate. □

We now use the last few results to prove our main theorem of this chapter.

Theorem 6.12 If A is a collection of AP's satisfying the conditions of notation 6.1 for some $k \geqslant 3$ and $n \geqslant 10$ and p_o is the least prime such that

$$p_o < \sum_{p \geqslant p_o} c(p),$$

then

(a) $$M(A) < \frac{A(p_o)}{A(k)} \; V(W(p_o),p_o)\, 2^n.$$

(b) Further, if $r = r(k,n)$ then

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

Proof: It follows from the fact that $\Sigma c(p) \geqslant 10$ and from inequality (3) that $p_o \geqslant 7$. We set

$$X = \sum_{p \geqslant p_o} c(p) \tag{11}$$

which implies $X < p_o$. We then have

$$1 - \sum_{p \geq p_o} c(p)/p \geq 1 - X/p_o > 0. \tag{12}$$

From (11) we have

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

Using this and (11) in corollary 6.4 (the use of which is justified by (12)) we obtain

$$M(A) < \frac{1 + X}{1 - X/p_o} \; 2^{n-X} \prod_{p<p_o} 2^{-c(p)} \; \frac{1 + c(p)}{1 - c(p)/p} .$$

We see by equation (2) that the product is not affected by factors corresponding to primes less than k. Applying corollary 6.8 to each of the other factors and using notation 6.5 we obtain

$$M(A) < 2^n \frac{A(p_o)}{A(k)} \; V(X,p_o). \tag{13}$$

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

$$p_o - 1 \geq X. \tag{14}$$

Next, let p_o' be the prime preceding p_o. By the definitions of X and p_o and by inequality (3),

$$p_o' \leq \sum_{p \geq p_o'} c(p)$$

$$\leq X + [\log_2 p_0']$$

Using notation 6.5, this and inequality (14) give

$$W(p_o) \leqslant X \leqslant p_o - 1. \tag{15}$$

Since X is an integer we have, by theorem 6.7,

$$V(X,p_o) \leqslant \max\{V(W(p_o),p_o),\ V(p_o-1,p_o)\} \tag{16}$$

Using lemma 6.6, theorem 6.7, the definition of $V(x,p)$ and the fact that $p_o \geqslant 7$ we obtain

$$\frac{V(W(p_o),p_o)}{V(p_o-1,p_o)} \geqslant \frac{V(p_o-4,p_o)}{V(p_o-1,p_o)}$$

$$= 2\,\frac{p_o-3}{p_o} > 1.$$

Thus the maximum in (16) is $V(W(p_o),p_o)$ and so by (13),

$$M(A) < \frac{A(p_o)}{A(k)}\, V(W(p_o),p_o)\, 2^n. \tag{17}$$

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

$$X = n - \sum_{p<p_o} c(p)$$

$$\geqslant n - \sum_{k\leqslant p<p_o} [\log_2 p].$$

Combining this with inequality (14) we obtain

$$p_o - 1 + \sum_{k\leqslant p<p_o} [\log_2 p] \geqslant n.$$

NOTE ADDED 1-5-86

One of the referees of this thesis has suggested that the inequality in Corollary 6.13 could be improved using results in the following papers.

H. Iwaniec, "On the problem of Jacobsthal", Demonstratio Math. 11(1978), 225-231.

H. Iwaniec, "Rosser's sieve", Acta Arith., 36(1980), 171-202.

It is hoped that this suggestion will be used in a forthcoming paper.

So that, using notation 6.5,

$$p_o \geqslant r(k,n).$$

Using this inequality and corollary 6.9 in (17) we obtain part (b) of the theorem. □

This theorem will be used in some applications in the next chapter. For others we use the following weaker but more convenient bound on $M(A)$.

Corollary 6.13 For A satisfying the conditions of notation 6.1 and $k \geqslant 4$ and $n \geqslant 10$ we have

$$M(A) \leqslant \frac{4}{9} \log 2\, n^3\, 2^{2n/3}/A(k).$$

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 (see notation 6.5)

$$M(A) < \frac{A(r)(1 + r' - [\log_2 r'])}{A(k)(r - r' + [\log_2 r'])}\, r\, 2^{-r' + [\log_2 r'] + n}$$

$$< \frac{A(r)(r')^2 r}{A(k)\log_2 r}\, 2^{-r'+n}$$

Using the estimates of lemma 6.10 and 6.11 we obtain the required inequality. □

CHAPTER 7

FINAL RESULTS ON THE CRITTENDEN AND VANDEN EYNDEN CONJECTURE AND DISCUSSION OF A NEW CONJECTURE

Having developed a sieve for the problem we now return to our investigation of the Crittenden and Vanden Eynden conjecture, conjecture 5.1. This chapter is divided into three sections. In the first we prove the conjecture in the case $k = 3$ and in the second we give upper bounds on the cardinality of minimal counterexamples for values of k greater than 3. The last section concerns a new conjecture which is analogous to conjecture 5.1. We show that this conjecture can be investigated using the methods of Chapter 5.

Section 1 : The case $k = 3$ of the conjecture

We prove the $k = 3$ case of the conjecture via a series of lemmas. The first enables us to use the results of Chapter 6 by showing that if A is a minimal counterexample then A satisfies the conditions of notation 6.1 with $k = 3$. That is,

A contains only AP's with prime moduli and each prime p is the modulus of $c(p)$ AP's in the collection,

(1)

$$|A| = n, \tag{2}$$

$$c(2) = 0, \tag{3}$$

$$c(p) \leqslant [\log_2 p] \quad \text{if} \quad p \geqslant 3. \tag{4}$$

The later lemmas show that no minimal counterexample exists with cardinality in certain intervals, the union of these intervals being the positive integers greater than 2.

Lemma 7.1 Let A be a minimal counterexample for $k = 3$. Then A satisfies conditions (1) to (4).

Proof: We show that all moduli occurring in A are odd. Suppose not and let

$$A_L = \{\langle a,d\rangle \in A : d \text{ is a power of } 2\}$$

$$A_G = \{\langle a,d\rangle \in A : d \text{ is a prime} \geqslant 3\}.$$

By corollary 5.12 $A_L \cup A_G = A$. Now let 2^α be the least power of 2 such that there exists an AP $\langle a,2^\alpha\rangle$ with

$$Z(A_L) \cap \langle a,2^\alpha\rangle = \phi.$$

Since A_L is assumed nonempty we must have $\alpha \geqslant 1$ and we may apply theorem 5.14 with $\langle a,2^\alpha\rangle$ in the role of $\langle a_o,d_o\rangle$. The first sum in the inequality is empty and so we have

$$|A_L| < \log_2 2^\alpha = \alpha.$$

We now apply theorem 3.9 to A_L and obtain

$$|A_L| \geqslant g(2^\alpha) = \alpha.$$

The contradiction implies that A_L is empty, so that $A = A_G$, and by corollary 5.15 A_G satisfies conditions (1) to (4). □

Lemma 7.2 If A is a minimal counterexample for $k = 3$ which does not cover 0 then

$$A = n \leqslant 15.$$

Since A is a counterexample we have, using notation 6.3

$$M(A) \geqslant 3(2^{n-2}).$$

If n were greater than 9 we could apply theorem 6.12, and obtain

$$A(r)V(W(r),r) \geqslant 3A(3)/4$$
$$= 3/2 . \qquad (5)$$

Here A, V, W and $r = r(3,n)$ are defined in notation 6.5. By corollary 6.9 the expression on the left is decreasing with r for $r \geqslant 5$, and by referring to the definition of $r(k,n)$ we see that r is non-decreasing with n. Now for $n = 16$ we have

$$r(3,16) = 13$$
$$W(13) = 8$$
$$V(8,13) = (117/5)2^{-8}$$
$$A(13) = (77)2^{-4}.$$

So that

$$A(13)V(W(13),13) = (9009/5)2^{-12} < 3/2$$

which contradicts (5). Thus $n < 16$ and we are done. □

Lemma 7.3 Let A be a minimal counterexample for $k = 3$ which does not cover 0. Then $|A|$ does not belong to the interval $[10,15]$.

Proof: Suppose A is a minimal counterexample for $k = 3$ which does not cover 0, and let p_o be the least prime such that

$$p_o > \sum_{p \geq p_o} c(p). \tag{6}$$

If $p_o \geq 13$ we obtain a contradiction as in lemma 7.2 using part (a) of theorem 6.12. Also, as in that theorem we have

$$p_o \geq r(3,n)$$
$$= 11$$

for n in the interval $[10,15]$. Thus we may assume $p_o = 11$ and apply corollary 6.4. Letting

$$X = \sum_{p \geq p_o} c(p)$$

this gives, since $c(2) = 0$ by (3),

$$M(A) < 11 \frac{1 + X}{11 - X} \prod_{2<p<11} \frac{1 + c(p)}{1 - c(p)/p}. \tag{7}$$

We call the product on the right hand side $Z(c(3),c(5),c(7))$. For a given value of

$$n - X = c(3) + c(5) + c(7)$$

there are a finite number of values that Z can take. The maximum of these values for each permissible value of $n - X$ is given in Table I.

$n - X$	Maximum of $Z(c(3),c(5),c(7))$
0	$Z(0,0,0) = 1$
1	$Z(1,0,0) = 3$
2	$Z(1,1,0) = 15/2$
3	$Z(1,1,1) = 35/2$
4	$Z(1,2,1) = 35$
5	$Z(1,2,2) = 63$

Table I Maxima of the function Z defined in lemma 7.3

n	X	Upper bound for M(A)	$3(2^{n-2})$
10	5	693	768
11	6	970.2	1,536
12	7	1,386	3,072
13	10	2,117.5	6,144
14	10	4,235	12,288
15	10	7,623	24,576

Table II Upper bounds for M(A) obtained from part (a) of theorem 6.12

By (6) and the fact that

$$c(3) + c(5) + c(7) \leqslant 5$$

we see that for each n in our interval

$$n - 5 \leqslant X \leqslant 10.$$

For each n we use table I to find the value of X in the range above which maximises the right hand side of (7). Hence we find upper bounds for $M(A)$. These are given in table II together with the relevant values of X and $3(2^{n-2})$. In each case we see that

$$M(A) < 3(2^{n-2})$$

contrary to our assumption that A is a counterexample. □

Lemma 7.4 Let A be a minimal counterexample for $k = 3$ which does not cover 0. Then $|A|$ does not belong to the interval [6,9].

Proof: We set

$$c_1 = c(3),\ c_2 = c(5),\quad N = 3(2^{n-2}).$$

For $c_2 \neq 2$ we use part (c) of theorem 6.2. With c_1 and c_2 fixed it is not hard to check that the right hand side of the inequality in that part is minimised when

$$\sum_{p>5} c(p)/p$$

is maximised, (this is not so when $c_2 = 2$). This occurs when $c(7)$ takes the maximum value allowed by (4), and similarly for higher primes until we have

$$\Sigma c(p) = n.$$

Table III gives the lower bounds for

$$|\{m : 1 \leqslant m \leqslant 3(2^{n-2}),\ m \notin Z(A)\}|$$

corresponding to the 4 possible assignments of values to the ordered pair $\{c_1,c_2\}$. In each case the lower bound is positive, contradicting the assumption that A is a counterexample.

n	$\{c_1,c_2\}$ =	{0,0}	{0,1}	{1,0}	{1,1}
6		15	11	9	4
7		25	21	16	10
8		37	36	28	22
9		56	55	46	44

Table III Lower bounds for $|\{m : 1 \leqslant m \leqslant 3(2^{n-2}),\ m \notin Z(A)\}|$ obtained from part (c) of theorem 6.2.

Suppose then that $c_2 = 2$, that is A contains two AP's with modulus 5. By hypothesis A does not cover 0 so neither of these is $<0,5>$. We now reduce A via $<0,5>$ to form a new collection A^* of $n-2$ AP's. By part (d) of corollary 2.12 we have

$$Z(A^*) \supseteq [1,[3(2^{n-2})/5]],$$

and we see that A^* contains only AP's with prime moduli not equal to 2 or 5, and with at most $[\log_2 p]$ AP's having modulus p. We now apply part (b) of theorem 6.2 setting $c_2 = 0$. We note that the right hand side of the inequality there is minimised when

$$\sum_{p>5} c(p)/p$$

is maximised and, as in the earlier part of the proof, we obtain lower bounds for

$$|\{m : 1 \leqslant m \leqslant [3(2^{n-2})/5], \quad m \notin Z(A^*)\}|.$$

For $n = 6,7,8$ and 9 these bounds are 0, 2, 1 and 1 respectively. That is, they are positive for $n = 7$, 8 and 9, contradicting the assumption that A is a counter-example to conjecture 5.1.

The only case left to check corresponds to $n = 6$ and $c_2 = 2$. If either of the following equations is not satisfied we obtain a positive bound using part (b) of theorem 6.2 as above.

$$c_1 = 1$$

$$c_3 = c(7) = 2.$$

Thus we assume these are satisfied together with $c_2 = 2$. Then $c_1 + c_2 + c_3 = 5$ so for some index $j > 3$ we have

$$c_j = 1$$

and

$$c_i = 0 \quad \text{for} \quad i > 3, \; i \neq j.$$

We now use part (c) of theorem 6.2 to obtain

$$|\{m : 1 \leqslant m \leqslant 3(2^{6-2}), \quad m \notin Z(A)\}|$$

$$\geq 4 - [48/p] + [48/3p] + 2[48/5p] - 2[48/15p]$$

$$= 4 - [48/p] + [48/3p].$$

This clearly increases with p and when $p = 11$ it equals 1. This contradicts the assumption that A is in a counterexample to conjecture 5.1, and we are done. □

Lemma 7.5 Let A be a minimal counterexample for $k = 3$ which does not cover 0. Then $|A|$ does not belong to the interval $[3,5]$.

Proof: The case $|A| = 3$ follows from theorem 5.8. For other values we use part (b) of theorem 6.2 with $3(2^{n-2})$ in the role of N and $c_1 = c(3)$, $c_2 = c(5)$ ... As in lemma 7.4 we obtain lower bounds for

$$|\{m : 1 \leq m \leq 3(2^{n-2}),\ m \notin Z(A)\}|$$

corresponding to the two possible values of c_1. These bounds are given in Table IV.

n	$c_1 = 0$	$c_1 = 1$
4	2	-1
5	3	1

Table IV Lower bounds for $|\{m : 1 \leq m \leq 3(2^{n-2}),\ m \notin Z(A)\}|$ obtained from part (b) of theorem 6.2.

These are strictly positive except in the case $n = 4$, $c(3) = 1$. Therefore if a minimal counterexample

exists for n less than 6 it must satisfy these conditions. To settle this final case we must show that if A is a collection of 4 AP's which satisfies conditions (1) to (4) and which contains exactly one AP with modulus 3, say $\langle a,3\rangle$, then

$$Z(A) \not\supseteq [1,12].$$

Suppose this is not so. We note that

$$\langle a,3\rangle \neq \langle 0,3\rangle,$$

(otherwise A would cover 0), so we may reduce A via $\langle 0,3\rangle$ to obtain a collection A^* of 3 AP's such that, by part (d) of corollary 2.12,

$$Z(A^*) \supseteq [0,3].$$

But each AP in A^* has modulus at least 5 and so can include at most one integer in this interval. Thus $Z(A^*)$ does not include $[1,4]$. This contradiction proves the lemma. □

Combining these four lemmas we prove the $k = 3$ case of conjecture 5.1.

Theorem 7.6 If A is a collection of n AP's where $n \geq 3$, each with modulus at least 3, and

$$Z(A) \supseteq [1,3(2^{n-2})]$$

then $Z(A) = \mathbb{Z}$.

Proof: The four preceding lemmas show that there is no minimal counterexample to the conjecture which covers 0. Hence by theorem 5.7 there is no minimal counter-example to conjecture 5.1 for $k = 3$, and this is our theorem. □

Section 2 : The cases $k > 3$ of the conjecture

In this section we give an upper bound for the cardinality of a minimal counterexample that does not cover 0 for arbitary values of $k \geqslant 4$. This means that the conjecture 5.1 could be verified for such values of k by checking that the conjecture holds for the low values of n, using methods similar to those used in the last section. We need to introduce some more notation.

Notation 7.7 Let A be a minimal counterexample that does not cover 0, then by corollary 5.12 each AP in A lies in one of the following collections.

$$A_L = \{\langle a,d\rangle \in A \ : \ d \text{ is a product of primes } < k\}$$

$$A_G = \{\langle a,d\rangle \in A \ : \ d \text{ is a prime } \geqslant k\}.$$

Let

$$|A_L| = n_L, \quad |A_G| = n_G.$$

Let P be the least modulus such that there exists an AP $\langle A,P\rangle$ with

$$\langle A,P\rangle \cap Z(A_L) = \phi.$$

Remark 7.8 It is easy to see, using lemma 2.1 part (a), that P divides $P(A_L)$, that is, P is a product of primes less than k.

Remark 7.9 We have two inequalities involving P. With g being the function defined in notation 3.8 we have, by theorem 3.9,

$$n_L \geqslant g(P), \tag{8}$$

and by theorem 5.14 with $\langle A,P\rangle$ in the role of $\langle a_o,d_o\rangle$ when $P \neq 1$, and by noting that $n_L = 0$ when $P = 1$, we have

$$n_L \leqslant \log_2 P. \tag{9}$$

We will need the following lemma.

Lemma 7.10 If P and A_L are as in notation 7.7, g is as in notation 3.8, $k \geqslant 4$,

(a) $\log_2 P - g(P) \geqslant 0$

(b) $\log_2 P - g(p) \leqslant \theta(k)/\log 2 - \pi(k)$

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

Proof: Part (a) is an immediate consequence of inequalities (8) and (9). For parts (b) and (c) we suppose P has prime factorisation

$$P = \prod_{i=1}^{t} p_i^{\alpha_i}.$$

Then,

$$\log_2 P - g(P) = \sum_{i=1}^{t} \left(\alpha_i \log_2 p_i - (\alpha_i - 1)(p_i - 1) - 1\right)$$

$$= \sum_{i=1}^{t} \left(\alpha_i (\log_2 p_i - p_i + 1) + p_i - 2\right).$$

The term in the inner brackets is $\leqslant 0$ for all primes p_i so the expression is maximised when each $\alpha_i = 1$. Thus by remark 7.8,

$$\log_2 P - g(P) \leqslant \sum_{p<k} (\log_2 p - 1)$$

$$\leqslant \theta(k)/\log 2 - \pi(k),$$

as required. This proves part (b) of the lemma.

For part (c) we obtain

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

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 5.17. This leads to

$$3 \log_2 P - 2g(P)$$

$$\leqslant \lceil \log_2 k \rceil (3 \log_2 2 - 2) + \left(1 + \lceil \log_3 k \rceil\right)(3 \log_2 3 - 4) +$$

$$2 + \sum_{3<p<k} (3 \log_2 p - 2)$$

$$\leqslant \lceil \log_2 k \rceil + (3 \log_2 3 - 4) \lceil \log_3 k \rceil + 3\theta(k)/\log 2 - 2\pi(k) - 1,$$

as required.

□

We now prove our theorem. This is our main result on the Crittenden and Vanden Eynden conjecture.

Theorem 7.11 If A is a minimal counterexample to conjecture 5.1 for some $k \geq 4$, then n is less than

$$3(\theta(k)/\log 2 + k) - 2\pi(k) + 21 \log_2 k + \lceil \log_2 k \rceil + (3 \log_2 3 - 4)\lceil \log_3 k \rceil - 4.$$

Proof: By theorem 5.7 we may assume, without loss of generality, that A does not cover 0. We use notation 7.7. Since

$$Z(A_L) \cap \langle A,P \rangle = \phi$$

we must have

$$Z(A_G) \supseteq \langle A,P \rangle \cap [1,k2^{n-k+1}].$$

Reducing A_G via $\langle A,P \rangle$ we obtain, by ideas similar to those in part (d) of corollary 2.12, a collection A^*_G which satisfies conditions (1) to (4) and such that $Z(A^*_G)$ contains $[k2^{n-k+1}/P]$ consecutive integers. As in the proof of theorem 5.7 we may form another collection A^{**}_G, say, which also satisfies conditions (1) to (4) and for which, using notation 6.3,

$$M(A^{**}_G) \geq [k2^{n-k+1}/P].$$

We use this to obtain an upper bound for n_G in terms of k and P. We first assume $n_G \geq 10$.

From corollary 6.13 we then have

$$\frac{4}{9} \log 2 \; n_G^3 \; 2^{2n_G/3}/A(k) > k2^{n-k+1}/P - 1.$$

Noting that

$$n = n_G + n_L, \tag{10}$$

and rearranging we obtain

$$\frac{4}{9} \log 2 \; n_G^3 \; 2^{-n_G/3} > kA(k)2^{-k+1+n_L-\log_2 P} - A(k)2^{-n_G}. \tag{11}$$

We claim that this implies

$$n_G < 3(k - 1 - n_L + \log_2 P + 7 \log_2 k). \tag{12}$$

To show this suppose that this inequality does not hold. Then, for $k \geqslant 4$ and using inequality (9) we see that $n_G \geqslant 24$. For such n_G the left hand side of (11) is decreasing, so it is sufficient to consider the value of the left hand side of (11) when

$$n_G = 3(k - 1 - n_L + \log_2 P + 7 \log_2 k).$$

We find, using inequality (8), part (b) of lemma 7.10 and this value of n_G that,

$$\frac{4}{9} \log 2 \; n_G^3 \; 2^{-n_G/3}$$

$$\leqslant 12 \log 2(k-1+\theta(k)/\log 2 - \pi(k) + 7 \log_2 k)^3 k^{-7} \; 2^{-k+1+n_L-\log_2 P}.$$

Now

$$12 \log 2(k-1+\theta(k)/\log 2 - \pi(k) + 7\log_2 k)^3 k^{-8}$$

is decreasing with k, and when $k = 4$ it equals $0.69016\ldots$ and so

$$\frac{4}{9} \log 2\, n_G^3\, 2^{-n_G/3} < k2^{-k+1+n_L-\log_2 P}$$

and is certainly less than the right hand side of (11). This establishes inequality (12) in the case $n_G \geqslant 10$.

If $n_G < 10$ it is easy to see that inequality (12) still holds using our assumption that $k \geqslant 4$ and inequality (9).

We now obtain our bound on n.

Using (10), (8) and (12) we have

$$\begin{aligned} n &< 3(k - 1 - n_L + \log_2 P + 7 \log_2 k) + n_L \\ &\leqslant 3k - 3 + 21 \log_2 k + 3 \log_2 P - 2g(P). \end{aligned}$$

Applying part (c) of lemma 7.10 gives the inequality of the theorem. □

Remark 7.12 Using the well known fact that $\theta(k) \sim k$, as $k \to \infty$, we see that as $k \to \infty$ our bound on n is asymptotically equal to

$$3(1/\log 2 + 1)k = (7.32808\ldots)k.$$

Section 3 : A new Conjecture

We have mentioned several times the following two questions asked by Erdös about regular covering systems with distinct moduli.

I Do such covering systems exist with all moduli arbitarily large?

II Do such covering systems exist with all moduli relatively prime to the first n primes?

Conjecture 5.1 is akin to question I in that it concerns collections of AP's having moduli at least k. In this section we make and investigate a conjecture which is similarly akin to question II. We first introduce a function $N(p,n)$.

Definition 7.13 Let n be an integer, p a prime and

$$n = n_o(p-1) + r, \quad 0 \leqslant r \leqslant p-2, \tag{13}$$

then

$$N(p,n) = (r+1)p^{n_o}. \tag{14}$$

We note that then

$$N(p,n+1) = (r+2)p^{n_o} \tag{15}$$

which holds even when $r = p-2$.

We can now make our new conjecture.

Conjecture 7.14 If p is a prime, A a collection of n AP's such that $P(A)$ is not divisible by any prime less than p and

$$Z(A) \supseteq [1,N(p,n)]$$

then

$$Z(A) = \mathbb{Z}.$$

If this conjecture is true then it is best possible in the sense of the following theorem.

Theorem 7.15 Conjecture 7.14 would be false if $N(p,n)$ were replaced with a smaller integer.

Proof: It is sufficient to present a collection that satisfies

$$|A| = n$$

$$Z(A) \supseteq [1,N(p,n) - 1]$$

$$Z(A) \neq \mathbb{Z}$$

and such that no modulus occurring in A is divisible by a prime less than p. It is not hard to see that the following is such a collection. Using the notation of equation (13),

$$A = \{\langle ip^{j-1},p^{j}\rangle : i = 1,\ldots, p-1, j = 1,\ldots,n_o\}$$

$$\cup \{\langle ip^{n_o},p^{n_o+1}\rangle : i = 1,\ldots,r\}.$$

Here the second bracketed collection is empty if $r = 0$.

□

Definition 7.16 A collection A that contradicts conjecture 7.14 is called a minimal counterexample to conjecture 7.14 for some prime p if $|A|$ is minimal over the set of all such counterexamples, and if the sum of the moduli occurring in A is minimal over all counterexamples with this cardinality.

Theorem 7.17 If a minimal counterexample to conjecture 7.14 exists for some value of p then a minimal counterexample exists which does not cover 0.

Proof: Similar to that of theorem 5.7. □

Theorem 7.18 If A is a counterexample to conjecture 7.14 then $|A| > p$.

Proof: Clearly A contains only AP's with modulus $\geqslant p$. If $|A|$ were less than p we would then have

$$M(A) \leqslant |A| - 1$$

contradicting the assumption that A is a counterexample. The case $|A| = p$ may be excluded using the method of theorem 5.8. □

In the rest of this section we will show that a minimal counterexample to this conjecture which does not cover 0 must satisfy a set of constraints which are similar to those obtained for conjecture 5.1 in Chapter 5. We begin with the following lemma.

Lemma 7.19 If A is a minimal counterexample to conjecture 7.14 for some prime p and q is a prime at least p then

$$Z(A) \not\equiv \mathbb{Z} \setminus \langle b,q \rangle \tag{16}$$

for any residue class b modulo q.

Proof: The proof is analogous to that of theorem 5.11. As in that proof, if (16) did not hold we could form a collection A^* with

$$|A^*| \leqslant n - q + 1$$

$$Z(A^*) \geq \left[1, \left[\frac{1}{q} N(p,n)\right]\right],$$

and such that $P(A^*)$ is not divisible by any prime less than p. To obtain a contradiction we must show that A^* is a counterexample to conjecture 7.14. To do this it is sufficient to show

$$N(p,n)/q \geqslant N(p,n-q+1) \tag{17}$$

This is slightly more complicated than the corresponding step in the proof of theorem 5.11 because of the awkward nature of the function N. We show that the function $mN(p,n-m+1)$ is decreasing for fixed n and increasing values of m for $m \geqslant p$. Let

$$n - m = n_o(p-1) + r, \quad 0 \leqslant r \leqslant p-2.$$

Using equation (15) we have

$$mN(p,n-m+1) = m(r+2)p^{n_o}$$

$$= \frac{m(r+2)}{(m+1)(r+1)} (m+1)N(p,n-(m+1)+1)$$

$$\geqslant (m+1)N(p,n-(m+1)+1)$$

for values of $m \geqslant p$. Thus the function decreases as required. Since we have assumed $q \geqslant p$ we therefore have

$$qN(p,n-q+1) \leqslant pN(p,n-p+1). \qquad (18)$$

It is easy to check that

$$pN(p,n-p+1) = N(p,n).$$

Combining this observation with (18) gives inequality (17) and we are done. □

Theorem 7.20 If A is a minimal counterexample to conjecture 7.14 then each modulus occurring in A is a prime.

Proof: Suppose A is a minimal counterexample for some p and

$$A = A^* \cup \{<a,qd>\}$$

where q is a prime at least p. We will show that

$$A^* \cup \{<a,q>\}$$

is also a counterexample to the conjecture which would contradict the minimality of A unless $d = 1$. Clearly

$$Z(A^* \cup \{<a,q>\}) \supseteq Z(A),$$

and

$$|A^* \cup \{\langle a,q\rangle\}| = |A|.$$

It is therefore sufficient to show that our new collection does not cover the integers. By lemma 7.19

$$Z(A) \not\equiv \mathbb{Z} \setminus \langle a,q\rangle.$$

Hence,

$$Z(A^* \cup \langle a,q\rangle) \neq \mathbb{Z}$$

as required. □

Our final result, analogous to corollary 5.15, gives an upper bound on the number of AP's occurring in a minimal counterexample to conjecture 7.14 which have modulus q.

Lemma 7.21 Let A be a minimal counterexample to conjecture 7.14, for some prime p, which does not cover 0 and let

$$|\{\langle a,d\rangle \in A : d = q\}| = c(q)$$

then

$$qN(p,n-c(q)) > N(p,n).$$

We reduce A via $\langle 0,q\rangle$ to obtain a collection A^*. As in the proof of theorem 5.12 we find

$$|A^*| \leqslant n - c(q)$$

$$Z(A^*) \supseteq [1,[N(p,n)/q]]$$

and no AP in A^* is divisible by a prime less than p. Since A is minimal we therefore have

$$[N(p,n)/q] < N(p,n-c(q))$$

which implies the required inequality. □

Theorem 7.22 With the notation of lemma 7.21

$$c(q) < \min\{q-1, \lceil \log q/\log p \rceil (p-1)\}.$$

Since A is minimal we may assume that all AP's with modulus q are distinct. Therefore, if $c(q) \geqslant q-1$ we would have

$$Z(A) \supseteq \mathbb{Z} \setminus \langle a,q \rangle$$

for some residue class a modulo q. This contradicts lemma 7.19.

On the other hand, if

$$c(q) \geqslant \lceil \log q/\log p \rceil (p-1)$$

we would have

$$N(p,n-c(q)) \leqslant p^{-\lceil \log q/\log p \rceil} N(p,n)$$

$$\leqslant q^{-1} N(p,n)$$

which contradicts lemma 7.21. These two contradictions prove the theorem. □

The result in this theorem is the best possible for some values of p,q and n, but not for all. Together theorems 7.20 and 7.22 give a fairly sharp characterisation of a minimal counterexample to conjecture 7.14. It should be possible to construct a sieve as in Chapter 6 and

thereby obtain an upper bound on the cardinality of a minimal counterexample as was done for conjecture 5.1 in the early part of this chapter.

BIBLIOGRAPHY

[1] V. Billik and H.M. Edgar, "Covering sets of congruences", Math. Mag. 46(1973), 265-270.

[2] N. Burshtein, "On natural exactly covering systems of congruences having moduli occurring at most twice", J. Number Th. 8(1976), 251-259.

[3] N. Burshtein, "On natural exactly covering systems of congruences having moduli occurring at most N times", Discrete Math. 14(1976), 205-214.

[4] 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.

[5] R.B. Crittenden and C.L. Vanden Eynden, "The union of arithmetic progressions with differences not less than k", Am. Math. Monthly, 79(1972), 630.

[6] H. Davenport, "The Higher Arithmetic", Hutchinson's University Library, Hutchinson House, London (1952), p. 57.

[7] P. Erdös, "On integers of the form $2^k + p$ and some related problems", Summa Brasil. Math. 2(1950), 113-123.

[8] P. Erdös, "On a problem concerning systems of congruences", (Hungarian, English Summary), Mat. Lapok 3(1952), 122-128.

[9] P. Erdös, "Remarks on Number Theory IV : extremal problems in number theory I", (Hungarian, English summary), Mat. Lapok 13(1962), 241-243.

[10] P. Erdös, "Problems and results in number theory in "Recent Progress in Number Theory", edited by H. Halberstam and C. Hooley, Academic Press (1981).

[11] R.K. Guy, "Unsolved Problems in Number Theory", Springer-Verlag (1980), 140-141.

[12] Hua Loo Keng, "Introduction to Number Theory", Springer-Verlag (1982), p. 29.

[13] I. Korec, "On a generalisation of Mycielski's and Znam's conjectures about coset decomposition of Abelian groups", Fund. Math. 85(1974), 41-48.

[14] I. Korec, "Improvement of Mycielski's inequality for nonnatural disjoint covering systems of Z", unpublished.

[15] W.J. Leveque, "Fundamentals of Number Theory", Addison-Wesley (1977).

[16] J. Mycielski and W. Sierpinski, "Sur une propriété des ensembles linéaires", Fund. Math. 58 (1966), 143-147.

[17] J. Nagura, "On the interval containing at least one prime number", Proc. Japan Acad. 28(1952), 177-181.

[18] S. Porubský, "Natural exactly covering systems of congruences", Czechoslovak Math. J. 24(1974), 598-606.

[19] S. Porubský, "Results and problems on covering systems of residue classes", Mitteilungen aus dem Mathem. Seminar Giessen, Heft 150, Giessen 1981.

[20] G. Barkley Rosser and L. Schoenfeld, "Approximate formulas for some functions of prime numbers", Illinois J. Math. 6(1962), 64-94.

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

[22] J.E. Shockley, "Introduction to Number Theory", Holt, Rinehart and Winston (1967).

[23] S.K. Stein, "Unions of arithmetic sequences", Math. Ann. 134(1958), 289-294.

[24] S. Znam, "On Mycielski's problem on systems of arithmetical progressions", Coll. Math. 15(1966), 201-204.

[25] S. Znam, "A remark to a problem of J. Mycielski on arithmetic sequences", Coll. Math. 20(1969), 69-70.

[26] S. Znam, "On properties of systems of arithmetic sequences", Acta Arith. 26(1975), 279-283.

[27] S. Znam, "On a relation between exactly covering systems and rooted trees", unpublished, referred to in [3].