

SOME COMBINATORIAL THEOREMS
WITH AN APPLICATION TO
A PROBLEM IN NUMBER THEORY

CENTRE FOR NEWFOUNDLAND STUDIES

**TOTAL OF 10 PAGES ONLY
MAY BE XEROXED**

(Without Author's Permission)

BENJAMIN I. GARDNER

14307





SOME COMBINATORIAL THEOREMS
WITH AN APPLICATION TO
A PROBLEM IN NUMBER THEORY

by



BENJAMIN I. GARDNER

A THESIS
SUBMITTED TO THE COMMITTEE ON GRADUATE STUDIES
IN PARTIAL FULFILLMENT OF THE REQUIREMENTS
FOR THE DEGREE OF
MASTER OF ARTS

MEMORIAL UNIVERSITY OF NEWFOUNDLAND
ST. JOHN'S, NEWFOUNDLAND

JUNE, 1967

(1)

ABSTRACT

The main object of this thesis is to study the following extremal problem in number theory: Let n and k be integers satisfying $n \geq k \geq 3$. Denote by $f(n,k)$ the largest positive integer for which there exists a set S of $f(n,k)$ integers satisfying

- (i) $S \subseteq \{ 1, 2, \dots, n \}$ and
- (ii) no k numbers in S have pairwise the same greatest common divisor.

We investigate the behaviour of $f(n,k)$ in the case where $k \rightarrow \infty$ with n . In particular we obtain estimates for $f(n, [\log^\alpha n])$ for fixed $\alpha > 0$ and $f(n, [n^\alpha])$ for fixed α , $0 < \alpha < 1$.

In the course of our investigations we make use of certain intersection theorems for systems of finite sets. We also include a number of new results concerning these theorems.

ACKNOWLEDGEMENTS

I would like to take this opportunity to express my sincere thanks to my supervisor, Dr. H.L. Abbott, for his invaluable assistance throughout the preparation of this thesis and to Mrs. Janet Buchanan for typing the manuscript.

TABLE OF CONTENTS

	<u>Page</u>
ABSTRACT	(i)
ACKNOWLEDGEMENTS	(ii)
CHAPTER I: INTRODUCTION	1
CHAPTER II: INTERSECTION THEOREMS FOR SYSTEMS OF SETS	
§2.1 Proof of the Erdős-Rado Theorem	3
§2.2 Lower bounds for $\phi(n, k)$	5
§2.3 Exact values of $\phi(n, k)$	10
§2.4 Some unsolved problems concerning $\phi(n, k)$	12
CHAPTER III: AN EXTREMAL PROBLEM IN NUMBER THEORY	
§3.1	14
APPENDIX	22
BIBLIOGRAPHY	33

CHAPTER I

INTRODUCTION

The main object of this thesis is to study the following extremal problem in number theory: Let n and k be integers satisfying $n \geq k \geq 3$. Denote by $f(n,k)$ the largest positive integer for which there exists a set S of $f(n,k)$ integers satisfying

(i) $S \subseteq \{1, 2, \dots, n\}$ and

(ii) no k numbers in S have pairwise the same greatest common divisor.

The determination of $f(n,k)$ appears to be a difficult problem and at the present time the existing upper and lower bounds for $f(n,k)$ are quite far apart. The various papers that have appeared on the subject have been devoted primarily to the obtaining of estimates for $f(n,k)$ for small fixed k and large n . In this thesis we investigate the behaviour of $f(n,k)$ in the case where $k \rightarrow \infty$ with n . Our results, however, are by no means complete and much work still remains to be done.

In the course of our investigations we make use of certain results concerning a combinatorial theorem of Erdős and Rado [4]. The Erdős-Rado theorem can be formulated as follows: Let n and k be positive integers with $k \geq 3$. Then there exists a least integer $\phi(n,k)$ such that if \mathcal{F}

is a family of more than $\phi(n,k)$ sets, each set with n elements, then some k members of \mathcal{F} have pairwise the same intersection. That this theorem is closely related to the number-theoretic problem formulated above can be seen as follows: Let $\mathcal{F} = \{ A_1, A_2, \dots, A_t \}$ be a family of distinct sets, no k of which have pairwise the same intersection. Let $A_1 = \{ a_1, a_2, \dots, a_e \}$ and let P_1, P_2, \dots, P_e be distinct primes. Then among the t numbers N_1, N_2, \dots, N_t , where $N_i = \prod_{a_j \in A_i} P_j$, there do not exist k numbers which have pairwise the same greatest common divisor. On the other hand if k members of \mathcal{F} have pairwise the same intersection then k of the numbers N_1, N_2, \dots, N_t will have pairwise the same greatest common divisor.

In Chapter II of this thesis we present a survey of the known results concerning the Erdős-Rado theorem. In addition we include a number of new results. In Chapter III we return to our main problem, discuss some of the known results and present some new results on the behaviour of $f(n,k)$.

CHAPTER II

INTERSECTION THEOREMS FOR SYSTEMS OF SETS

§2.1 Proof of the Erdős-Rado Theorem

We devote this section to the proof of the theorem of Erdős and Rado stated in Chapter I. Let $\{T_n\}_{n=1}^{\infty}$ be the sequence defined as follows

$$(2.1.1) \quad T_1 = k-1, \quad T_n = (k-1) n T_{n-1} - (k-1)(n-1) \text{ for } n \geq 2.$$

Then

Theorem 2.1.1 If \mathcal{F} is a family of $T_n + 1$ distinct sets, each set with n elements, then some k members of \mathcal{F} have pairwise the same intersection.

Proof: The theorem is true for all k when $n = 1$. Assume that it is true for all k when the number of elements in each set of \mathcal{F} is $\leq n-1$. If an element b appears in at least $T_{n-1} + 1$ members of \mathcal{F} we may delete this element to get a family of $T_{n-1} + 1$ sets, each set with $n-1$ elements. By the induction hypothesis some k of these sets have pairwise the same intersection. Reinserting b gives a family of $T_{n-1} + 1$ sets, each set with n elements, and some k of these having pairwise the same intersection. Hence we may assume that no element appears in more than T_{n-1} sets.

Let $A_1 \in \mathcal{F}$. Let $\mathcal{F}_1 = \{F : F \in \mathcal{F}, F \cap A_1 \neq \emptyset\}$. Then

$|\mathcal{F}_1| \leq n T_{n-1} - (n-1)$. Let $\mathcal{F}_1^* = \mathcal{F} - \mathcal{F}_1$. Then $A_1 \cap F = \emptyset$

for $F \in \mathcal{F}_1^*$ and $|\mathcal{F}_1^*| \geq (k-2) n T_{n-1} - (k-2)(n-1) + 1$. Let

$A_2 \in \mathcal{F}_1^*$. Then $A_1 \cap A_2 = \emptyset$. Let $\mathcal{F}_2 = \{F : F \in \mathcal{F}_1^*, F \cap A_2 \neq \emptyset\}$.

Then $|\mathcal{F}_2| \leq n T_{n-1} - (n-1)$. Let $\mathcal{F}_2^* = \mathcal{F}_1^* - \mathcal{F}_2$. Then

$A_2 \cap F = \emptyset$ for $F \in \mathcal{F}_2^*$ and $|\mathcal{F}_2^*| \geq (k-3) n T_{n-1} - (k-3)(n-1) + 1$.

Let $A_3 \in \mathcal{F}_2^*$. Then $A_1 \cap A_2 = A_1 \cap A_3 = A_2 \cap A_3 = \emptyset$. Repeat this

process. At stage $k-1$ we have sets A_1, A_2, \dots, A_{k-1} such

that $A_i \cap A_j = \emptyset$, $1 \leq i < j \leq k-1$, and a family \mathcal{F}_{k-1}^* such

that $A_i \cap F = \emptyset$ for $i=1, 2, \dots, k-1$ and every $F \in \mathcal{F}_{k-1}^*$ and

$|\mathcal{F}_{k-1}^*| \geq 1$. Let A_k be any set in \mathcal{F}_{k-1}^* . Then

$A_i \cap A_j = \emptyset$ for $1 \leq i < j \leq k$. This completes the proof of the theorem.

It follows from theorem 2.1.1 that $\phi(n, k)$ exists and satisfies

$$(2.1.2) \quad \phi(n, k) \leq T_n$$

and

$$(2.1.3) \quad \phi(n, k) \leq (k-1) n \phi(n-1, k) - (k-1)(n-1).$$

Moreover, one can show easily by induction on n , that (2.1.3) implies

$$(2.1.4) \quad \phi(n,k) \leq n! (k-1)^n \left\{ 1 - \sum_{t=1}^{n-1} \frac{t}{(t+1)! (k-1)^t} \right\}.$$

The upper bound for $\phi(n,k)$ given by (2.1.4) has not in general been improved, but some known values of $\phi(n,k)$ indicate that this result is not best possible. We shall return to this in section 2.3 where we discuss some known values of $\phi(n,k)$.

§2.2 Lower bounds for $\phi(n,k)$

Theorem 2.2.1 For all positive integers a, b and k , with $k \geq 3$, we have:

$$(2.2.1) \quad \phi(a+b, k) \geq \phi(a, k) \phi(b, k).$$

Proof Let $\mathcal{F}_a = \{A_1, A_2, \dots, A_{\phi(a,k)}\}$ and $\mathcal{F}_b = \{B_1, B_2, \dots, B_{\phi(b,k)}\}$ be families of sets having the desired property (that is, no k of the A 's and no k of the B 's have pairwise the same intersection). As the notation implies, each A has a elements and each B has b elements. We also take for granted that $A_i \cap B_j = \emptyset$ for all i and j . Let $\mathcal{F} = \{A_i \cup B_j : i=1, 2, \dots, \phi(a,k), j=1, 2, \dots, \phi(b,k)\}$. It is clear that the number of sets in \mathcal{F} is $\phi(a,k)\phi(b,k)$ and that each member of \mathcal{F} has $a+b$ elements. The proof of the theorem will be complete if we show that no k members of \mathcal{F} have pairwise the same intersection.

Suppose there exist distinct sets F_1, F_2, \dots, F_k in \mathcal{F} and a set $S \subset \cup \mathcal{F}$ such that

$$(2.2.2) \quad F_i \cap F_j = S, \quad i, j = 1, 2, \dots, k, \quad i \neq j.$$

Let $F_i = A_{m_i} \cup B_{n_i}$ for $i=1, 2, \dots, k$. Partition the elements of S into two sets S_1 and S_2 , an element being placed in S_1 if it belongs to $\cup \mathcal{F}_a$ and in S_2 if it belongs to $\cup \mathcal{F}_b$. Then it is not difficult to see, using (2.2.2) that

$$(2.2.3) \quad A_{m_i} \cap A_{m_j} = S_1, \quad i, j = 1, 2, \dots, k, \quad i \neq j.$$

and

$$(2.2.4) \quad B_{n_i} \cap B_{n_j} = S_2, \quad i, j = 1, 2, \dots, k, \quad i \neq j.$$

If the sets $A_{m_1}, A_{m_2}, \dots, A_{m_k}$ are all distinct, or if the sets

$B_{n_1}, B_{n_2}, \dots, B_{n_k}$ are all distinct, then we have a contradiction.

Hence two of the A_{m_i} must be identical and two of the B_{n_i} must be identical. Thus in view of (2.2.3) and (2.2.4), we have

$$A_{m_1} = A_{m_2} = \dots = A_{m_k} \quad \text{and} \quad B_{n_1} = B_{n_2} = \dots = B_{n_k}.$$

Hence $F_1 = F_2 = \dots = F_k$. This contradicts the fact that the F 's were chosen as distinct subsets of \mathcal{F} . The proof of the theorem is now complete.

Theorem 2.2.1 and the fact that $\phi(1, k) = k-1$ implies that

$$(2.2.5) \quad \phi(n, k) \geq (k-1)^n.$$

This result was obtained by Erdős and Rado, but by a different argument. It is clear, however, that any improvement on (2.2.5) for a fixed value of n will automatically yield a better lower bound for $\phi(n, k)$ for all larger values of n . With this

in mind we turn our attention to the derivation of a new lower bound for $\phi(2,k)$. We prove

Theorem 2.2.2

$$(2.2.6) \quad \phi(2,k) \geq \begin{cases} (k-1)^2 + \frac{k-2}{2}, & \text{if } k \text{ is even} \\ k(k-1), & \text{if } k \text{ is odd.} \end{cases}$$

Proof We first take the case where k is even and let

$k = 2\ell$. Let

$$\mathcal{F}_1 = \{(i,j) : i = 1, 2, \dots, \ell; j = 2\ell + 1, \dots, 4\ell - 1\}$$

$$\mathcal{F}_2 = \{(i,j) : i = \ell + 1, \dots, 2\ell - 1; j = 3\ell, \dots, 4\ell - 1\}$$

$$\mathcal{F}_3 = \{(i,j) : \ell + 1 \leq i < j \leq 2\ell\}$$

$$\mathcal{F}_4 = \{(i,j) : 2\ell \leq i < j \leq 3\ell - 1\}.$$

Then clearly

$$|\mathcal{F}_1| = \ell(2\ell - 1)$$

$$|\mathcal{F}_2| = \ell(\ell - 1)$$

$$|\mathcal{F}_3| = |\mathcal{F}_4| = \binom{\ell}{2}.$$

Let $\mathcal{F} = \mathcal{F}_1 \cup \mathcal{F}_2 \cup \mathcal{F}_3 \cup \mathcal{F}_4$. Since the families $\mathcal{F}_1, \mathcal{F}_2, \mathcal{F}_3,$

and \mathcal{F}_4 are disjoint we have $|\mathcal{F}| = |\mathcal{F}_1| + |\mathcal{F}_2| + |\mathcal{F}_3| + |\mathcal{F}_4|$

$$= \ell(2\ell - 1) + \ell(\ell - 1) + 2\binom{\ell}{2}$$

$$= (k-1)^2 + \frac{k-2}{2}.$$

It is not difficult to check that if $1 \leq t \leq 4\ell - 1$ then t appears in at most $k-1$ members of \mathcal{F} . Hence if k members of \mathcal{F} are to have pairwise the same intersection they must be pairwise disjoint. This contradicts the fact that

$2k = 4l > 4l-1 = |\cup \mathcal{F}|$. This completes the proof for k even.

We now take the case of k being odd and let $k = 2l + 1$. Let

$\mathcal{F}_1 = \{(i, j) : 1 \leq i < j \leq k\}$. Then $|\mathcal{F}_1| = \binom{k}{2}$.

$\mathcal{F}_2 = \{(i, j) : k+1 \leq i < j \leq 2k\}$. Then $|\mathcal{F}_2| = \binom{k}{2}$.

Let $\mathcal{F} = \mathcal{F}_1 \cup \mathcal{F}_2$. Then $|\mathcal{F}| = |\mathcal{F}_1| + |\mathcal{F}_2| = \binom{k}{2} + \binom{k}{2} = k(k-1)$.

To complete the proof we need to show that no k members of \mathcal{F} have pairwise the same intersection. Now each of $1, 2, \dots, 2k$ appears in $k-1$ members of \mathcal{F} . Hence if k sets are to have pairwise the same intersection they must be pairwise disjoint, but this would contradict the fact that $2(l+1) > 2l + 1 = k = |\cup \mathcal{F}_1| = |\cup \mathcal{F}_2|$. Hence no k sets have pairwise the same intersection. The proof of the theorem is now complete.

Theorem 2.2.3

$$(2.2.7) \quad \phi(n, k) \geq \begin{cases} \phi(2, k)^{\frac{n}{2}}, & \text{if } n \text{ is even} \\ (k-1)\phi(2, k)^{\frac{n-1}{2}}, & \text{if } n \text{ is odd.} \end{cases}$$

Proof This theorem can be easily proved by using (2.2.1) and iterating.

It is clear that (2.2.6) and (2.2.7) will yield a better lower bound for $\phi(n, k)$ than that given by (2.2.5) for all $k \geq 3$ and $n \geq 2$.

The preceding three theorems, with the exception of the second part of theorem 2.2.2, which is new, were proved by H.L. Abbott [2].

While the known upper and lower bounds for $\phi(n,k)$ are quite far apart, we can still gain a little more insight into the behaviour of $\phi(n,k)$. We prove the following theorem which was brought to the attention of H.L. Abbott in a written correspondence from P. Erdős.

Theorem 2.2.4 For fixed values of k $\lim_{n \rightarrow \infty} \phi(n,k)^{\frac{1}{n}}$ exists.

Proof For a fixed k we denote $\phi(n,k)$ by $\phi(n)$ and let $\alpha = \liminf_{n \rightarrow \infty} \phi(n)^{\frac{1}{n}} \leq \limsup_{n \rightarrow \infty} \phi(n)^{\frac{1}{n}} = \beta$.

It follows easily from (2.2.1) that

$$(2.2.8) \quad \phi(bl) \geq \phi(l)^b.$$

Suppose first that $\beta < \infty$. Let $\epsilon > 0$ be given. Let l be the least positive integer for which

$$(2.2.9) \quad \phi(l)^{\frac{1}{l}} > \beta - \epsilon.$$

Let $n = bl + r$, $0 \leq r \leq l - 1$. Then $\phi(n) = \phi(bl+r) \geq \phi(bl)$.

$$\text{Hence } \phi(n)^{\frac{1}{n}} = \phi(bl+r)^{\frac{1}{bl+r}} \geq \phi(bl)^{\frac{1}{bl+r}}$$

$$= \phi(bl)^{\frac{1}{bl} \left(\frac{1}{1+r/bl} \right)} > (\beta - \epsilon)^{\frac{1}{1+r/bl}}$$

where we have used (2.2.8) and (2.2.9).

Hence $\alpha = \liminf_{n \rightarrow \infty} \phi(n)^{\frac{1}{n}} \geq \beta - \epsilon$.

Since ϵ is arbitrary we have $\alpha = \beta$.

The case where $\beta = \infty$ can be disposed of in a very similar manner. Let N be a positive number and let ℓ be the least integer for which $\phi(\ell)^{\frac{1}{\ell}} > N$. Then if $n = b\ell + r$, $0 \leq r \leq \ell - 1$ we get, by the same argument used above,

$$\phi(n)^{\frac{1}{n}} > N^{1/1 + \frac{r}{b\ell}}$$

It follows that $\alpha \geq N$ and hence that $\alpha = \infty$.

This completes the proof of the theorem.

§2.3 Exact values of $\phi(n,k)$

It is obvious that $\phi(1,k) = k-1$ for all values of k . Erdős and Rado [4] observed that

Theorem 2.3.1

$$(2.3.1) \quad \phi(2,3) = 6$$

Proof That $\phi(2,3) \leq 6$ follows from (2.1.4) and it is not difficult to see that in the family $\{(1,2), (1,3), (2,3), (4,5), (4,6), (5,6)\}$ no three sets have pairwise the same intersection.

Up to the present these were the only known values of $\phi(n,k)$ and the evaluation of $\phi(n,k)$ for larger

values of n and k seems to be a very difficult problem. However, we have been able to evaluate $\phi(2,4)$ and $\phi(3,3)$. We state the results and some consequences, but since the proofs are somewhat long we do not present them here. A sketch of the argument used is found in the Appendix.

Theorem 2.3.2

$$(2.3.2) \quad \phi(2,4) = 10.$$

Note that (2.1.4) yields only $\phi(2,4) \leq 15$.

Corollary

$$(2.3.3) \quad \phi(n,4) \leq n! 3^n \left\{ \frac{5}{9} - \frac{1}{9} \sum_{t=2}^{n-1} \frac{t}{(t+1)! 3^{t-2}} \right\}.$$

Proof This follows easily from (2.1.3) and (2.3.2).

Theorem 2.3.3

$$(2.3.4) \quad \phi(3,3) = 20.$$

Note that (2.1.4) yields only $\phi(3,3) \leq 32$.

Corollary

$$(2.3.5) \quad \phi(n,3) \leq n! 2^n \left\{ \frac{5}{12} - \frac{1}{8} \sum_{t=3}^{n-1} \frac{t}{(t+1)! 2^{t-3}} \right\}.$$

Proof This follows easily from (2.1.3) and (2.3.4).

Any result of this type will not improve the general upper bound by more than a constant factor. However, Theorem 2.3.3 together with (2.2.1) yields a

substantially better lower bound for $\phi(n,3)$. We have the following

Corollary

$$(2.3.6) \quad \phi(n,3) \geq c(20)^{\frac{n}{3}}.$$

§2.4 Some unsolved problems concerning $\phi(n,k)$

In this section we state some unsolved problems and make some brief statements about them.

1. Does there exist an absolute constant c , such that $\phi(n,k) \leq c^n (k-1)^n$?

Erdős and Rado [4] conjectured that such a constant does exist.

2. Let $A_1, A_2, \dots, A_{\phi(n,k)}$ be sets, no k of which have pairwise the same intersection and let $A = \bigcup_{i=1}^{\phi(n,k)} A_i$.

Can one give bounds for $|A|$ in terms of n, k or $\phi(n,k)$?
What other information could one give concerning the structure of A ?

3. Can the existence of $\phi(n,k)$ be established solely by using a special case of Ramsey's Theorem [7], which can be formulated as follows?

Let t and $k \geq 3$ be positive integers. Then there exists a least positive integer $h(t,k)$ such that if G is a complete graph with more than $h(t,k)$ vertices and if the edges of G are colored in any way in k colors

then there results a complete subgraph of G with k vertices all of whose edges have the same color.

Let $\{A_1, A_2, \dots, A_{\phi(n,k)}\}$ be a family of sets such that each set has n elements and no k of the sets have pairwise the same intersection. Form all possible intersections $A_i \cap A_j$, $i \neq j$, and denote the family of distinct intersections by $\{I_1, I_2, \dots, I_t\}$. Let G be a complete graph with vertices $P_1, P_2, \dots, P_{\phi(n,k)}$. Color the edges of G in t colors C_1, C_2, \dots, C_t by coloring the edge joining P_i and P_j color C_r if $A_i \cap A_j = I_r$. Then a simple argument shows that G contains no complete subgraph on k vertices all of whose edges have the same color. It follows that

$$(2.4.1) \quad h(t, k) \geq \phi(n, k).$$

In proving (2.4.1) we are making use of the fact that $\phi(n, k)$ exists. Can one use Ramsey's Theorem to prove the existence of $\phi(n, k)$?

CHAPTER III

AN EXTREMAL PROBLEM IN NUMBER THEORY

§3.1

For the convenience of the reader we restate the problem here. Let n and k be positive integers with $n \geq k \geq 3$. Denote by $f(n,k)$ the largest positive integer for which there exists a set S of $f(n,k)$ integers satisfying

- (i) $S \subseteq \{1, 2, \dots, n\}$ and
- (ii) no k members of S have pairwise the same greatest common divisor.

The problem of determining $f(n,k)$ appears to be difficult and at the present time all known upper and lower bounds for $f(n,k)$ are quite far apart. P. Erdős [3] proved that there is an absolute constant $c > 1$ such that for every $\epsilon > 0$ and every fixed k .

$$(3.1.1) \quad c^{\frac{\log n}{\log \log n}} < f(n,3) \leq f(n,k) \leq n^{\frac{3}{4} + \epsilon}$$

provided $n \geq n_0(k, \epsilon)$. H.L. Abbott [2] proved that for every $\epsilon > 0$ and every fixed k and m

$$(3.1.2) \quad f(n,k) > \left\{ \phi(m,k) \right\}^{\frac{\log n}{(m+\epsilon) \log \log n}}$$

provided $n \geq n_0(k, m, \epsilon)$

We now investigate partially the case where $k \rightarrow \infty$ with n . We prove the following theorems:

Theorem 3.1.1 Let $\alpha > 0$ and $\epsilon > 0$ be given. Then

$$(3.1.3) \quad n^{\frac{\alpha}{1+\alpha} - \epsilon} < f(n, [\log^n n]) < n^{\frac{2\alpha+3}{2\alpha+4} + \epsilon}$$

provided $n \geq n_0(\alpha, \epsilon)$.

Theorem 3.1.2 Let $t \geq 2$ be an integer. Then

$$(3.1.4) \quad f(n, [n^{\frac{1}{t}}]) > \frac{(1-\epsilon)n}{(\log n)^t}$$

for every $\epsilon > 0$ provided $n \geq n_0(t, \epsilon)$.

To prove theorems 3.1.1 and 3.1.2 we need the following lemma:

Lemma Let t and k be positive integers and let P_1, P_2, \dots, P_{tk} be the first tk primes. (P_r denotes the r^{th} prime). Let S_t be the set of the k^t numbers $P_{i_1} P_{i_2} \dots P_{i_t}$ where $(s-1)k+1 \leq i_s \leq sk$ for $s=1, 2, \dots, t$.

Then no $k+1$ members of S_t have pairwise the same greatest common divisor.

Proof The lemma is obviously true when $t=1$.

Assume that the lemma holds for all positive integers $\leq t$. Suppose S_{t+1} has $k+1$ members A_1, A_2, \dots, A_{k+1} which have pairwise the same greatest common divisor. Let

$A_i = N_i P'_i$, where $N_i \in S_t$ and the P'_i are primes satisfying

$$P'_{tk+1} \leq P'_1 \leq P_{(t+1)k}. \quad \text{Let } (A_1, A_2) = (A_1, A_3) = \dots = (A_k, A_{k+1}) = d \text{ (say).}$$

Since there are $k+1$ primes P'_1 chosen from a set of k primes these cannot all be distinct. Suppose, without loss of generality, that $P'_1 = P'_2$. Then $P'_1 \mid (A_1, A_2)$ and hence $P'_1 \mid d$. Hence $P'_1 \mid (A_i, A_j)$ for each $i, j = 1, 2, \dots, k+1$. But P'_1 is different from any prime divisor of any number in S_t . Thus $P'_1 = P'_2 = \dots = P'_{k+1}$. Hence N_1, N_2, \dots, N_{k+1} are all different and have pairwise the greatest common divisor $\frac{d}{P'_1}$.

But this contradicts the fact that no $k+1$ members of S_t have pairwise the same greatest common divisor.

Thus no $k+1$ members of S_{t+1} have pairwise the same greatest common divisor. This proves the lemma.

Observe that the largest number in S_t is

$$N = P_{k^2k} P_{2k} \dots P_{tk}. \quad \text{We thus have}$$

$$(3.1.5) \quad f(N, k+1) \geq k^t.$$

We now prove Theorem 3.1.2. Let $t \geq 2$ be a fixed

positive integer and set $k = \left\lceil \frac{1}{n^{\frac{1}{t}}} \log n \right\rceil$. Then by the Prime Number Theorem ($P_r \sim r \log r$, [6] p.10) we have

$$\begin{aligned} N &= \prod_{m=1}^t P_{mk} \sim \prod_{m=1}^t mk \log mk \sim t! (k \log k)^t \\ &= t! \left(\left\lceil \frac{1}{n^{\frac{1}{t}}} \log n \right\rceil \log \left\lceil \frac{1}{n^{\frac{1}{t}}} \log n \right\rceil \right)^t < t! \left(\frac{1}{n^{\frac{1}{t}}} \right)^t \leq \frac{n}{2}. \end{aligned}$$

Hence, for all sufficiently large n , we have

$$(3.1.6) \quad N < n,$$

also

$$(3.1.7) \quad k^t = \left[\frac{\frac{1}{n^{\frac{1}{t}}}}{\log n} \right]^t > \left(\frac{\frac{1}{n^{\frac{1}{t}}}}{\log n} - 1 \right)^t > \frac{(1-\epsilon)n}{(\log n)^t}$$

provided $n \geq n_0(t, \epsilon)$.

Now (3.1.5), (3.1.6) and (3.1.7) imply

$$f(n, [n^{\frac{1}{t}}]) \geq f(N, [n^{\frac{1}{t}}]) \geq f(N, k+1) \geq k^t \geq \frac{(1-\epsilon)n}{(\log n)^t}.$$

This establishes (3.1.4) and Theorem 3.1.2 is proved.

To obtain the lower bound in (3.1.3) choose

$$k = \left[\log^\alpha n \right] - 1 \text{ and } t = \left[\frac{\log n}{(1+\alpha) \log \log n} \right].$$

Then for all sufficiently large n , we have

$$(3.1.8) \quad \begin{aligned} N &= \prod_{m=1}^t P_{mk} < (1+\epsilon) \prod_{m=1}^t mk \log mk \\ &< (1+\epsilon)^t t! k^t \prod_{m=1}^t \log mk \\ &< (1+\epsilon)^t t! k^t (\log tk)^t < n. \end{aligned}$$

Also, since $(\log^\alpha n)^{\frac{\log n}{(1+\alpha) \log \log n}} = (e^{\alpha \log \log n})^{\frac{\log n}{(1+\alpha) \log \log n}}$

$= e^{\frac{\alpha}{1+\alpha} \log n} = n^{\frac{\alpha}{1+\alpha}}$, then for sufficiently large n , we have

$$(3.1.9) \quad k^t > n^{\frac{\alpha}{1+\alpha} - \epsilon}.$$

Now (3.1.5), (3.1.8) and (3.1.9) yield

$$f(n, [\log^\alpha n]) \geq f(N, k+1) \geq k^t \geq n^{\frac{\alpha}{1+\alpha} - \epsilon}.$$

This establishes the lower bound in (3.1.3).

In order to obtain the upper bound given in (3.1.3) we use a modification of the argument used by Erdős to obtain the upper bound given by (3.1.1).

Let $\{a_1, a_2, \dots, a_\ell\}$ be an arbitrary subset of

$$\{1, 2, \dots, n\}, \text{ where } \ell = \left[n^{\frac{2\alpha+3}{2\alpha+4} + \epsilon} \right].$$

Split the a 's into two classes. In the first class put those a 's which have at least $\left[\frac{\log n}{2(2+\alpha)\log \log n} \right] = u$ distinct prime factors. Denote by w_1, w_2, \dots the squarefree integers not exceeding n which have exactly u prime factors. Every number of the first class is a multiple of some w_i , hence the number of integers of the first class is at most

$$\sum_i \frac{n}{w_i} < n \frac{\left(\sum_{P_i \leq n} \frac{1}{P_i} \right)^u}{u!} < \frac{n(\log \log n + B)^u}{u!}$$

where B is a constant (see [6] p.351). Stirling's formula for $u!$ and some straightforward calculations show that

$\sum_i \frac{n}{w_i} < \frac{1}{2} n^{\frac{2\alpha+3}{2\alpha+4} + \epsilon}$ for every $\epsilon > 0$ if n is sufficiently large.

Hence the number of integers of the second class

is greater than $\frac{1}{2} n^{\frac{2\alpha+3}{2\alpha+4} + \epsilon}$.

Consider the unique factorization

$$(3.1.10) \quad a_i = A_i B_i, \quad (A_i, B_i) = 1,$$

where each prime factor of A_i occurs with an exponent greater than one and B_i is squarefree. It is known [5] that the number of integers $m \leq n$ all of whose prime factors occur with an exponent greater than one is less than $c n^{\frac{1}{2}}$, where c is a constant. Hence there are at least

$\frac{1}{2c} n^{\frac{\alpha+1}{2\alpha+4} + \epsilon}$ integers a_{i_j} with the same A_i . That is, we have

$$(3.1.11) \quad a_{i_j} = A_{i_j} B_{i_j}, \quad 1 \leq j \leq r,$$

$$r > \frac{1}{2c} n^{\frac{\alpha+1}{2\alpha+4} + \epsilon}, \quad A_{i_j} = A.$$

Now the number of prime factors of the squarefree number B_i is less than u . For all sufficiently large n , we have

$$\frac{1}{2c} n^{\frac{\alpha+1}{2\alpha+4} + \epsilon} > u! [\log^\alpha n]^u.$$

Hence from (2.1.4) and the basic principle stated in Chapter I there are at least $[\log^\alpha n]$ B's and hence by (3.1.11) at least $[\log^\alpha n]$ a's which have pairwise the same greatest common divisor. This proves the upper bound in (3.1.3) and completes the proof of Theorem 3.1.1.

It would be nice to prove $f(n, [\log^\alpha n]) = n^{h(\alpha)+o(1)}$ and determine $h(\alpha)$. However, we could not do it.

A paper based on this chapter has been accepted for publication in the Canadian Mathematical Bulletin. The referee of the paper suggested the following improvement on Theorem 3.1.2

Theorem 3.1.3 Let $0 < \alpha < 1$. Then $f(n, [n^\alpha]) = (1+o(1))c_\alpha n$, where c_α is a constant depending only on α .

Proof. It is well known that the number of integers $\leq n$ all of whose prime factors are $\leq n^\alpha$ is $(1+o(1))c_\alpha n$, (c_α is a continuous function of α). This set of integers clearly does not contain a subset of $2 + \pi(n^\alpha)$ terms which have pairwise the same greatest common divisor. Hence

$$(3.1.12) \quad f(n, [n^\alpha]) > f(n, \pi(n^\alpha)+2) = (1+b(1))c_\alpha n.$$

Next we show that if $1 \leq a_1 < \dots < a_k < n$, $k > (c_\alpha + \epsilon)n$, then there is a subsequence $a_{i_1} < \dots < a_{i_r}$, $r > n^\alpha$ any two terms of which have the same greatest common divisor. By the continuity of c_α as a function of α there is an $\eta = \eta(\epsilon)$ and a subsequence $a_{j_1} < \dots < a_{j_s}$, $s > \eta n$, so that the greatest prime factor p_{j_u} of a_{j_u} , $1 \leq u \leq s$ is greater than $n^{(\alpha + \epsilon/2)}$.

Now consider the numbers $b_u = a_{j_u} / p_{j_u}$, $b_u < n^{1 - \alpha - \epsilon/2}$,

$1 \leq u \leq s$, $s > \eta n$. Thus there is a d so that $b_u = d$ has more than $\eta n^{\alpha + \epsilon/2} > n^\alpha$ solutions and this d is the greatest common divisor in question. It follows from this that

$$(3.1.13) \quad f(n, [n^\alpha]) < (c_\alpha + \epsilon) n$$

and hence it follows from (3.1.12) and (3.1.13) that

$$f(n, [n^\alpha]) = (1 + o(1)) c_\alpha n.$$

APPENDIX

In this appendix we outline the proofs of theorems 2.3.2 and 2.3.3 which were stated in Chapter II.

Theorem 2.3.2

$$\phi(2,4) = 10.$$

Proof That $\phi(2,4) \geq 10$ follows from (2.2.6). To prove that $\phi(2,4) \leq 10$ we consider any family of 11 sets, each set with 2 elements. We assume that no 4 of these sets have pairwise the same intersection and wish to get a contradiction.

Clearly, we may assume that no element appears in more than 3 sets. If there are n_1 elements which appear exactly once, n_2 elements which appear exactly twice, and n_3 elements which appear exactly 3 times then

$$(1) \quad n_1 + 2n_2 + 3n_3 = 22.$$

Suppose 2 elements a, b appear exactly once and appear together, that is, in the same set. Then by (1) there must be at least one element c which appears at most twice.

We have at worst

$$(\underline{ab})(\underline{cd})(c-)(d-)(d-)(\underline{ef})(e-)(e-)(f-)(f-)(\underline{\underline{\quad}})$$

where the underlined sets are pairwise disjoint. Hence we

may assume that if 2 elements appear exactly once they do not appear together.

Suppose 2 elements a, b appear exactly once and we have $(ac), (bd)$ where $c \neq d$. Replace (ac) by (bc) . Then if the resulting family is to have 4 sets with pairwise the same intersection these sets must include (bc) and must be pairwise disjoint. That is $(bc), (pq), (rs),$ and (tu) are pairwise disjoint. Thus c does not appear among p, q, r, s, t, u . Moreover a does not appear among p, q, r, s, t, u since a appears only once in the original family. Hence $(ac), (pq), (rs),$ and (tu) are pairwise disjoint. Hence if elements a and b appear exactly once we must have $(ac), (bc)$. It also follows from this that if a, b, c appear exactly once we must have $(ad), (bd), (cd)$ and that there cannot be 4 or more elements which appear exactly once.

There are thus four cases to be considered:

- (1) 3 elements a, b, c appear exactly once in which case we have $(ad), (bd), (cd)$
- (2) 2 elements a, b appear exactly once in which case we have $(ac), (bc)$
- (3) 1 element appears exactly once
- (4) no element appears exactly once.

We present the details of the argument for case 1 only.

Case 1 If 3 elements a, b, c appear exactly once then, by (1), we have one of

- (a) 2 elements each appear exactly twice
- (b) 5 elements each appear exactly twice.

Case 1(a) Suppose 2 elements d, e each appear exactly twice. Then by (1) there are 5 elements f, g, h, k, m say, each of which appears exactly 3 times. At worst we have one of

- (i) $(\underline{af})(bf)(cf)(\underline{de})(dg)(e-)(\underline{gh})(g-)(h-)(h-)(\underline{\underline{--}})$
- (ii) $(\underline{af})(bf)(cf)(\underline{dg})(dh)(eg)(\underline{eh})(g-)(h-)(\underline{\underline{--}})$
- (iii) $(\underline{af})(bf)(cf)(\underline{dg})(dh)(\underline{ek})(eg)(g-)(k-)(k-)(\underline{\underline{--}})$
- (iv) $(af)(bf)(cf)(dg)(dh)(ek)(em)(g-)(g-)(pq)(rs).$

where in cases (i), (ii) and (iii) the underlined sets are pairwise disjoint. In (iv) we take (af) , (dg) one of (ek) , (em) and one of (pq) , (rs) since one of k, m does not appear in one of (pq) , (rs) .

Case 1(b) Suppose 5 elements d, e, f, g, h each appear exactly twice. Then by (1) there are 3 elements k, m, n each of which appears exactly 3 times. Clearly two of d, e, f, g, h say d and e , must appear together. Moreover one of f, g, h , say f , does not appear with d or e . At worst we

have

(ak)(bk)(ck)(de)(d-)(e-)(fm)(f-)(m-)(m-)(--).

Cases 2, 3, and 4 can be disposed of in a very similar manner.

We turn our attention now to the proof that $\phi(3,3) = 20$. The proof depends heavily on the following

Lemma

(a) Let \mathcal{F} be a family of 6 sets, each set with 2 elements, no 3 members of \mathcal{F} having pairwise the same intersection.

Then

$$\mathcal{F} = \{(ab), (ac), (bc), (de), (df), (ef)\}.$$

(b) Let \mathcal{F} be a family of 5 sets, each set with 2 elements, no 3 members of \mathcal{F} having pairwise the same intersection.

Then either

$$\mathcal{F} = \{(ab), (ac), (bc), (de), (df)\}$$

or

$$\mathcal{F} = \{(ab), (ac), (bd), (ce), (de)\}$$

Proof: (a) Let $\{(ab), (cd), (ef), (gh), (ij), (kl)\}$ be a family of sets having the desired property. Clearly no element appears in 3 or more sets. We may also assume that

no element appears in exactly one set, since if this were the case we would have three sets which are pairwise disjoint. We may therefore assume that each element appears in exactly two sets and in view of this we may assume, without loss of generality, that $a = c$ and $b = e$.

The case $d = f$ clearly leads to a family whose structure is the same as that given in the statement of the lemma. We may therefore assume $d \neq f$ and also without loss of generality that $d = g$. We then have

$$\{(ab), (ad), (bf), (dh), (ij), (kl)\}.$$

Now $f = h$ is impossible since it implies $(ij) = (kl)$. We may therefore assume $f = i$, say. Then $h = j$ is impossible since this would imply k and l appear once only. Hence we must have $h = k$ and $j = l$, say. The resulting family is

$$\{(ab), (ad), (bf), (dh), (fj), (hj)\}$$

in which 3 sets (ab) , (dh) and (fj) are pairwise disjoint. This completes the proof of the first part of the lemma.

The proof of part (b) is similar and will therefore be omitted.

Now we prove

Theorem 2.3.3 $\phi(3,3) = 20.$

Proof That $\phi(3,3) \geq 20$ follows from the fact that in the following family of sets, no 3 sets have pairwise the same intersection:

{(abc), (abd), (ace), (adf), (aef), (bcf), (bde),
(bef), (cde), (cdf), (mnp), (mnq), (mpr), (mqs), (mrs),
(nps), (nqr), (nrs), (pqr), (pqs)}.

To show that $\phi(3,3) \leq 20$ we consider an arbitrary family \mathcal{F} of 21 sets each with 3 elements. We have to show that 3 of the sets have pairwise the same intersection.

It is clear that if an element appears in more than 6 members of \mathcal{F} there is no problem. Hence we may assume that each element appears in at most 6 sets. Also if no element appears in more than 4 members of \mathcal{F} we have, at worst,

(abc) (a--) (a--) (a--) (b--) (b--) (b--) (c--) (c--)
(c--) (def) (d--) (d--) (d--) (e--) (e--) (e--) (f--)
(f--) (f--) (---)

where the underlined sets are pairwise disjoint.

The importance of the lemma now becomes clear. If an element a appears in 6 sets then these sets are completely determined and in fact must be

(abc) (abd) (acd) (aef) (aeg) (afg).

In addition, if an element a appears in exactly 5 sets we must have one of

(a) $(abc)(abd)(acd)(aef)(aeg)$

(b) $(abc)(abd)(acf)(ade)(aef)$.

Suppose (abc) is a member of \mathcal{F} and that a, b and c each appear in 6 sets. Then we must have

$$\mathcal{F}_1 = \{(abc), (abd), (acd), (aef), (aeg), (afg), (bcd), (bpq), (bpr), (bqr), (cxy), (cxz), (cyz)\}$$

as a sub family of \mathcal{F} . If e, f, p, q, x, y are all different the sets $(aef), (bpq)$ and (cxy) are pairwise disjoint. Hence without loss of generality we may assume $e = p$. If e, f, q, r, x, y are all different the sets $(aef), (bqr)$ and (cxy) are pairwise disjoint. Hence we may assume either $f = q$ or $f = x$ or $q = x$. If $f = q$ or $f = x$ then f appears in at most 2 members of $\mathcal{F} - \mathcal{F}_1$. Also e appears in at most 2 members of $\mathcal{F} - \mathcal{F}_1$ and d in at most 3. Thus, in view of the fact that $|\mathcal{F}_2| = 13$ there is one member of $\mathcal{F} - \mathcal{F}_1$ which does not contain any of a, b, c, d, e, f . This set and the sets (aef) and (bcd) are therefore pairwise disjoint. The case where $q = x$ can be disposed of in a very similar manner and we find that one member of $\mathcal{F} - \mathcal{F}_1$ and the sets (acd) and (beq) are pairwise disjoint.

The above discussion indicates the type of argument

that is to be used. We select a set (abc) in \mathcal{F} and specify the number of sets containing a , b , and c . Let

$\mathcal{F}_1 = \{F: F \in \mathcal{F}, F \cap (abc) \neq \emptyset\}$. The structure of \mathcal{F}_1 is then largely determined. We then show that either three members of \mathcal{F}_1 are pairwise disjoint or one member of $\mathcal{F} - \mathcal{F}_1$ and two members of \mathcal{F}_1 are pairwise disjoint.

We present the details of the argument in what is the most difficult case, namely, the case where a, b and c each appear in 5 sets. By the Lemma, \mathcal{F}_1 must be one of the following:

1. $\{(abc), (abd), (acd), (aef), (aeg), (bcd), (bpq), (bpr), (c--), (c--)\}$
2. $\{(abc), (abd), (acd), (aef), (aeg), (bcq), (bdr), (bqr), (c--), (c--)\}$
3. $\{(abc), (abd), (acd), (aef), (aeg), (bpq), (bpr), (bqr), (c--), (c--), (c--)\}$
4. $\{(abc), (abd), (ace), (adf), (aef), (bcd), (bpq), (bpr), (c--), (c--)\}$
5. $\{(abc), (abd), (ace), (adf), (aef), (bpq), (bpr), (bqr), (c--), (c--), (c--)\}$
6. $\{(abc), (abd), (ace), (adf), (aef), (bcq), (bdr), (bqr), (c--), (c--)\}$.

In case 1, d appears in at most 2 members of $\mathcal{F} - \mathcal{F}_1$, p appears in at most 3 and q in at most 4. Since $|\mathcal{F}_1| = 10$

there is a set in $\mathcal{F} - \mathcal{F}_1$ which does not contain any of a, b, c, d, p, q. This set and (acd) and (bpq) are therefore pairwise disjoint.

In case 2, d appears in at most 2 member of $\mathcal{F} - \mathcal{F}_1$ and q and r each appear in at most 3 members of $\mathcal{F} - \mathcal{F}_1$. Hence (acd), (bqr) and a set in $\mathcal{F} - \mathcal{F}_1$ are pairwise disjoint.

In case 3, d, p and q each appear in at most 3 members of $\mathcal{F} - \mathcal{F}_1$. Since $|\mathcal{F}_1| = 11$, (acd), (bpq) and a set in $\mathcal{F} - \mathcal{F}_1$ are pairwise disjoint.

In case 4, d appears in at most 2 members of $\mathcal{F} - \mathcal{F}_1$ and e and f each appear in at most 3. Hence (aef), (bcd) and a set in $\mathcal{F} - \mathcal{F}_1$ are pairwise disjoint.

In case 5, we observe first that e is different from at least two of p, q, r. Thus (ace) and (bpq), say, are disjoint. Also e, p, and q each appear in at most 3 members of $\mathcal{F} - \mathcal{F}_1$. Since $|\mathcal{F}_1| = 11$, (ace), (bpq) and a set in $\mathcal{F} - \mathcal{F}_1$ are pairwise disjoint.

Case 6 presents some additional difficulties and we must examine more closely those members of \mathcal{F}_1 which contain c. Suppose one of the sets containing c (other than (abc), (ace), (bcq)) does not contain d and let this set be (cxy). Then (abd) and (cxy) are disjoint. Now d appears in

at most 2 members of $\mathcal{F} - \mathcal{F}_1$ and x and y each appear in at most 4. Since $|\mathcal{F}_1| = 10$ there is a set in $\mathcal{F} - \mathcal{F}_1$ which is disjoint from (abd) and (cxy). Hence we may assume that d appears in the two hitherto unspecified sets containing c. If $f \neq q$ the sets (adf) and (bcq) are disjoint. Since d appears in at most 2 members of $\mathcal{F} - \mathcal{F}_1$ and f and q each appear in at most 3, there is a set in $\mathcal{F} - \mathcal{F}_1$ which is disjoint from (adf) and (bcq). We may therefore assume $f = q$. Similarly we may assume $e = r$. The lemma then shows that the two remaining sets containing c must be (cde) and (cdf). Hence we have

$$\mathcal{F}_1 = \{(abc), (abd), (ace), (adf), (aef), (bcf), (bde), (bfe), (cde), (cdf)\}.$$

Observe that every set in \mathcal{F}_1 is disjoint from every set in $\mathcal{F} - \mathcal{F}_1$. If no element appears in more than 4 members of $\mathcal{F} - \mathcal{F}_1$ then 2 members of $\mathcal{F} - \mathcal{F}_1$ are disjoint and we have finished. Hence we may assume there is an element p which appears in 5 members of $\mathcal{F} - \mathcal{F}_1$. By the lemma, 3 of the sets containing p must be of the form (pqr), (pq-), (pr-). If q or r appear in at most 4 sets then there is a set in $\mathcal{F} - \mathcal{F}_1$ which is disjoint from (pqr) and we have finished. Hence we may assume that each of q, r appear in 5 members of $\mathcal{F} - \mathcal{F}_1$. Let

$\mathcal{F}_2 = \{F: F \in \mathcal{F} - \mathcal{F}_1, F \cap (pqr) \neq \emptyset\}$. We can now treat \mathcal{F}_2 in exactly the same way that we have treated \mathcal{F}_1 . If cases

1 - 5 hold there are two sets in \mathcal{J}_2 which are disjoint and we have finished. Otherwise we have

$$\mathcal{J}_2 = \{(pqr), (pqs), (prt), (psv), (ptv), (qrv), \\ (qst), (qvt), (rst), (rsv)\}.$$

However we now have $(abc), (pqr)$ and the remaining member of $(\mathcal{J} - \mathcal{J}_1) - \mathcal{J}_2$ pairwise disjoint.

BIBLIOGRAPHY

1. Abbott, H.L., Some problems in combinatorial analysis. Ph.D. Thesis, University of Alberta, (1965), pp. 45-56.
2. Abbott, H.L., Some remarks on a combinatorial theorem of Erdős and Rado. Can. Math. Bull., Vol. 9, No. 2, (1966), pp. 155-160.
3. Erdős, P., On a problem in elementary number theory and a combinatorial problem. Math. of Comp., Vol. 18, No. 88, (1964), pp. 644-646.
4. Erdős, P. and R. Rado, Intersection theorems for systems of sets. Jour. Lon. Math. Soc., 35 (1960), pp. 85-90.
5. Erdős, P. and G. Szekeres, Über die Anzahl der Abelschen Gruppen gegebener Ordnung und über ein verwandtes zahlentheoretisches Problem. Acta Sci. Math. (Szeged), Vol. 7, 1934, pp. 94-102.
6. Hardy, G.H. and E.M. Wright, An Introduction to the Theory of Numbers, 4th. ed., Oxford University Press, London, (1959).
7. Ramsay, F.P., On a problem in formal logic. Proc. Lon. Math. Soc., 30 (1930), pp. 264-286.



