COLLOQUIA MATHEMATICA SOCIETATIS JÁNOS BOLYAI
4. COMBINATORIAL THEORY AND ITS APPLICATIONS, BALATONFÜRED (HUNGARY), 1969.

On the set of non pairwise coprime divisors of a number

by

P. Erdős and J. Schönheim
Budapest, Hungary Calgary, Canada

1. INTRODUCTION

The problems we will be talking about in this lecture arise from the idea of considering intersection theorems for finite sets and of generalizing them in the sense that the obtained theorems should hold for entities more general than sets.

Such entitites are, for example; the divisors of a given integer. It is amusing to observe that the symbol $S_n^{\ell}(N)$ - representing the number of divisors of N containing ℓ prime factors, where n denotes (redundantly) the number of prime factors of N- satisfies a large number of identities generalizing identities on binomial coefficients. In order to give a simple example let N have $p_1^{\alpha_1} p_2^{\alpha_2} \dots p_s^{\alpha_s}$ as its decomposition in primes, $\alpha_1+\alpha_2+\dots+\alpha_s = n$, then

$$(0) \qquad \sum_{i=0}^{n} S_n^i(N) = \prod_{i=1}^{s} (\alpha_i+1).$$

If $\alpha_1 = \alpha_2 = \dots = \alpha_s = 1$ then $S_n^i(N) = \binom{n}{i}$ and (0) generalizes $\sum_{i=0}^{n} \binom{n}{i} = 2^n$.

The first non-trivial result in this direction has been obtained [1] by De Bruijn, Van Tengbergen and Kruijswijk, and is a generalization of Sperner's theorem. One of us [2] generalised various theorems which are consequences of the same theorem.

Although the numbertheoretical language used in [1] and [2] is attractive for its simplicity and for its immediate applications, other authors prefer to consider more general concepts. Katona [3] proved theorems containing the results of [1] and [2] using integral valued functions on $S = \{x_1, x_2, \dots, x_n\}$ $(0 \le f(x_k) \le \alpha_k)$.

We might mention here, that a theorem in this more general framework is not always a translation of the corresponding theorem for sets, new facts make their appearance. For example if n different sets $A_1, A_2, \dots, A_n$ are given, then the number of different differences $A_i - A_j$ is $\ge n$, but if n different divisors $d_1, d_2, \dots, d_n$ of a positive integer are given then the number of different ratios $(d_i, d_j)/d_i$ these correspond to the differences above, is not necessarily $\ge n$. See [4].

2. RESULTS

We will now turn our attention to another intersection theorem [5], generalise it and reveal the new facts involved. The considered result of [5] is:

a'. If $A_1, A_2, \dots, A_m$ are distinct sets such that $|A_1 \cup A_2 \cup \dots \cup A_m| = n$ and $A_i \cap A_j \ne \phi$ for every i, j then $m \le 2^{n-1}$ and for every n there are $m = 2^{n-1}$ such sets.

b'. Moreover, if the sets $B_1, B_2, \dots, B_s$, $s < 2^{n-1}$ satisfy the requirements of a' then there exist sets $B_{s+1}, B_{s+2}, \dots, B_{2^{n-1}}$ such that the sets $B_1, B_2, \dots, B_{2^{n-1}}$ also satisfy these requirements.

The more general problem in the spirit of the introductory words of this talk is the following:

a^*. To determine a number $f(N)$ such that if $D_1, D_2, \dots, D_m$ are different divisors of N, and each two of the D's have a common divisor >1, then $m \le f(N)$ and there are, for every $N, m = f(N)$ such divisors.

b^*. Moreover, is it true that if $G_1, G_2, \dots, G_m$ are divisors of satisfying the requirements of a^* and $m < f(N)$ then there are divisors of N $G_{s+1}, \dots, G_{f(N)}$ such that $G_1, G_2, \dots, G_{f(N)}$ also satisfy these requirements?

The bound $f(N)$ is determined in the following theorem, whereas the answer to b^* is negative. In order to have an affirmative answer $f(N)$ is replaced in b^* by another value $g(N)$ which is best possible but is not very illuminating.

THEOREM 1.

If $D_1, \dots, D_m$ are different divisors of an integer N whose decomposition in prime factors is $\prod_{i=1}^{t} p_i^{\alpha_i}$ and each two of the D's have a common divisor >1 then, denoting $\prod_{i=1}^{t} \alpha_i = \alpha$

$$(1) \qquad \max m = f(N) = \frac{1}{2} \sum \max \left\{ \prod_{\nu=1}^{\mu} \alpha_{i_\nu},\ \alpha \Big/ \prod_{\nu=1}^{\mu} \alpha_{i_\nu} \right\}$$

where the summation is over all subsets $\{i_1, \dots, i_\mu\}$ of $\{1, \dots, t\}$ and for the empty subset the product is considered to be one. The result is best possible, for every N there are $f(N)$ divisor no two of which are relatively prime.

Denote by $F_i^{(t)}$ a family of 2^{t-1} subsets A_j, $1 \le j \le 2^{t-1}$ of $\{1, \dots, t\}$ where the intersection of any two A_j's is non-empty. Let $F_i^{(t)}$, $1 \le i \le s$ be the set of all these families. As far as we know the value of s is not known.

Trivially

$$2^{\frac{1}{2}\binom{n}{[\frac{n}{2}]}} < s < \binom{2^n}{2^{n-1}} .$$

Let $N = \prod_{i=1}^{t} p_i^{\alpha_i}$. Put

$$(2) \qquad g(N) = \min_{F_i^{(t)}} \sum \prod_{\nu=1}^{\mu_j} \alpha_{i_\nu}$$

where the minimum is to be taken over all the F_i, $1 \le i \le s$ and the summation is extended over all the 2^{t-1} A_j's of F_i, $A_j = \{i_1, \dots, i_\mu\}$.

THEOREM 2.

Let $G_1, \dots, G_m$ be m distinct divisors of N no two of which are relatively prime. Assume $m < g(N)$. Then there are $g(N) - m$ further divisors $G_{m+1}, \dots, G_{g(N)}$ so that no two of the $g(N)$ distinct divisors G_i, $1 \le i \le g(N)$ are relatively prime. Theorem 2 is best possible.

The proof utilizes the following lemma.

LEMMA

If $p_1, p_2, \dots, p_t$ are different primes and $\alpha_1, \alpha_2, \dots, \alpha_t$ are positive integers α_i depending only on p_i $(i = 1, 2, \dots, t)$ and if

$$\{i_1, i_2, \dots, i_\mu\} \cup \{j_1, j_2, \dots, j_{\mu'}\}$$

$$\{h_1, h_2, \dots, h_\sigma\} \cup \{k_1, k_2, \dots, k_{\sigma'}\}$$

are two different partitions of the index set $\{1, 2, \dots, t\}$ such that

$$(i) \qquad \alpha_{i_1} \alpha_{i_2} \cdots \alpha_{i_\mu} \ge \alpha_{j_1} \alpha_{j_2} \cdots \alpha_{j_{\mu'}},$$

and

(ii) $$\alpha_{h_1}\alpha_{h_2}\cdots\alpha_{h_\sigma} \geq \alpha_{k_1}\alpha_{k_2}\cdots\alpha_{k_\sigma},$$

then the greatest common divisor of $p_{i_1}p_{i_2}\cdots p_{i_\mu}$ and $p_{h_1}p_{h_2}\cdots p_{h_\sigma}$ is greater than 1.

3. PROOFS:

Proof of the Lemma.

Suppose the contrary; then $p_{h_1}p_{h_2}\cdots p_{h_\sigma}$ is a proper divisor of $p_{j_1}p_{j_2}\cdots p_{j_\mu}$, hence

$$\{\alpha_{h_1}, \alpha_{h_2}, \dots, \alpha_{h_\sigma}\} \subsetneqq \{\alpha_{j_1}, \alpha_{j_2}, \dots, \alpha_{j_\mu}\}$$

and (i) contradicts (ii).

PROOF OF THE THEOREM

Denote by M the square free part of N i.e. $M = p_1 p_2 \cdots p_t$ and by S a set of divisors of N, any two members of S having a common divisor >1, as required in $\mathfrak{a}^*$.

Let

(3) $$(p_{i_1}\cdots p_{i_\mu})(p_{j_1}\cdots p_{j_\mu})$$

be a factorization of M into two relatively prime factors, then S cannot contain integers composed from $p_{i_1},\dots,p_{i_\mu}$ and from $p_{j_1},\dots,p_{j_\mu}$, hence contains at most $\max\{\prod_{\nu=1}^{\mu}\alpha_{i_\nu}, \alpha/\prod_{\nu=1}^{\mu}\alpha_{i_\nu}\}$ members deriving from that factorization. This shows $|S| \leq f(N)$.

To show $|S| \geq f(N)$ consider all such factorizations (3) of M for which

(4) $$\prod_{i=1}^{\mu}\alpha_{i_\nu} \geq \alpha / \prod_{\nu=1}^{\mu}\alpha_{i_\nu}$$

and say $i_1 = 1$ if equality holds

Put in S all the $\prod_{\nu=1}^{\mu} \alpha_{i_\nu}$ integers $\prod_{\nu=1}^{\mu} p_{i_\nu}^{\beta_{i_\nu}}$, $1 \le \beta_{i_\nu} \le \alpha_{i_\nu}$; $\nu = 1, \dots, \mu$.

In this way we construct a set of divisors of N no two of which are relatively prime (by our Lemma) and containing

$$\sum \prod_{\nu=1}^{\mu} \alpha_{i_\nu} = \frac{1}{2} \sum \max \{ \prod_{i=1}^{\nu} \alpha_{i_\nu}, \alpha / \prod_{i=1}^{\mu} \alpha_{i_\nu} \}$$

members, where the second summation is as in (1), while the first is restricted to index subsets satisfying (4). This leads to $f(N)$ divisors for every N, which completes the proof of Theorem 1.

Now we prove Theorem 2. Let $G_1, \dots, G_m$, $m < g(N)$ be any m divisors of N no two of which are relatively prime. Put

$$G_j = \prod_{i=1}^{\mu_j} p_{i_\nu}^{\beta_\nu}, \quad 1 \le \beta_\nu \le \alpha_{i_\nu} ; \quad 1 \le j \le m .$$

No two of the G's are relatively prime. Thus any two of the m sets $\{ i_1, \dots, i_{\mu_j} \}$, $1 \le j \le m$ have a non-empty intersection, hence they all belong to the same $F^{(t)}$ say to $F_r^{(t)}$. But then one can clearly add to the set $G_1, \dots, G_m$ at least (the summation is extended over the 2^{t-1} sets A_j of $F_r^{(t)}$).

$$\sum \prod_{\nu=1}^{\mu_j} \alpha_{i_\nu} - m \ge g(N) - m$$

further divisors no two of which are relatively prime, which proves Theorem 2.

To show that Theorem 2.is best possible observe that if F_1 gives the minimum in (2) and we consider the $g(N)$ divisors (no two of which are relatively prime) $\prod_{i=1}^{\mu_j} p_{i_\nu}^{\beta_\nu}$, $1 \le \beta_\nu \le \alpha_{i_\nu}$; $1 \le j \le 2^{t-1}$ corresponding to the 2^{t-1} A's of F_1 clearly every further divisor of N is relatively prime to at least one of the given $g(N)$ divisors.

Unfortunately (2) is not a very useful and illuminating formula. It is easy to see that

$$g(N) \ge \alpha - 1 + \frac{1}{2} \sum \min \left\{ \prod_{i=1}^{\mu} \alpha_{i_\nu} , \alpha / \prod_{i=1}^{\mu} \alpha_{i_\nu} \right\} \tag{5}$$

where in (5) the summation is extended over all the subsets of $\{1, \ldots, t\}$ except the empty set and its complement $\{1, \ldots, t\}$.

Assume $\alpha_1 \ge \ldots \ge \alpha_t$, perhaps

$$g(N) = \alpha_t \prod_{i=1}^{t-1} (\alpha_i + 1) \tag{6}$$

F_1 would then consist of all the sets containing t .

REFERENCES

[1] DE BRUIJN, N.G., VAN E. TENGBERGEN, C.A., and KRUIJSWIJK, D. On the set of divisors of a number. Nieuw Arch. Wiskunde (2), 23 (1949-51), 191-193.

[2] SCHÖNHEIM, J., A generalization of results of P. ERDŐS, G. KATONA and D. KLEITMAN concerning Sperner's theorem. J. Combinatorial Theory (to appear)

[3] KATONA, G., A generalization of some generalizations of Sperner's Theorem. J. Combinatorial Theory (to appear).

[4] MARICA, J. and SCHÖNHEIM, J. Differences of sets and a problem of GRAHAM. Can. Math. Bull. (to appear)

[5] P. ERDŐS, CHAO KO and R. RADO, Intersection theorems for systems of finite sets, Quart. J. Math. 12 (1961), 313-320.