ON THE SET OF DIVISORS OF A NUMBER

MURRAY HOCHBERG
Brooklyn College (CUNY), Brooklyn, New York 11210

If z is a natural number and if $z = p_1^{\lambda_1} p_2^{\lambda_2} \cdots p_j^{\lambda_j}$ is its factorization into primes, then the sum $\lambda_1 + \lambda_2 + \cdots + \lambda_j$ will be called the *degree* of z. Let m be a squarefree natural number of degree n, i.e., m is the product of n different primes. Let the set of all divisors of m of degree k be denoted by D_k, $k = 0, 1, \cdots, n$; clearly, the cardinality of D_k is equal to $C(n,k)$, where $C(n,k)$ denotes the binomial coefficient, $n!/[k!(n-k)!]$. Two natural numbers δ and ζ are said to *differ in exactly one factor* if $\delta = rp_1$ and $\zeta = rp_2$, where p_1 and p_2 are prime numbers, with $p_1 \neq p_2$. Let α be a natural number that is a divisor of m. A natural number β is said to be an *extension* of α if β is a divisor of m, α is a divisor of β and the degree of β is one more than the degree of α. A natural number γ is said to be a *restriction* of α if γ is a divisor of m, γ is a divisor of α and the degree of γ is one less than the degree of α. If A is a non-empty set of divisors of m, we shall denote by A^+ the set of all extensions of the divisors in A; if $A = \phi$, we define $A^+ = \phi$. The cardinality of any set A will be denoted by $|A|$ and we use the superscript "c" to denote complementation.

In this note, the author gives a relatively short and interesting proof of the following theorem:

Theorem. Let A be a collection of divisors of a squarefree natural number m such that each divisor in A has degree k, $0 \leqslant k \leqslant n$. Then

$$|A^+| \geqslant \frac{|A|C(n,k+1)}{C(n,k)}, \tag{1}$$

and for $A \neq \phi$ equality holds if and only if $|A| = C(n,k)$.

Before proving the theorem, we need to prove one lemma that is also of independent interest.

Lemma. Let A be a non-empty collection of divisors of a squarefree natural number m such that each number in A has degree k, $0 < k < n$, and $|A| < C(n,k)$. Then there exists natural numbers $\alpha \in A$ and $\beta \in A^c \cap D_k$ such that α and β differ in exactly one factor.

Proof. Let ν_0 be an arbitrary number in A. Since $|A| < C(n,k)$, there exists a number $\delta \in A^c$ with the degree of δ equal to k. Let q be the greatest common divisor of ν_0 and of δ and let the degree of q be equal to ω. Then

$$\frac{\nu_0}{\delta} = \frac{t_1 t_2 \cdots t_{k-\omega}}{s_1 s_2 \cdots s_{k-\omega}}, \quad t_i \neq s_j,$$

where $i,j = 1, 2, \cdots, k-\omega$. We now define recursively a finite sequence of numbers by setting

$$\nu_j = \nu_{j-1}\left(\frac{s_j}{t_j}\right), \qquad j = 1, 2, \cdots, k-\omega.$$

Plainly, $\nu_j \in D_k$, ν_{j-1} and ν_j differ in exactly one factor and $\nu_{k-\omega} = \delta$. Since the first number in the sequence ν_0, $\nu_1, \cdots, \nu_{k-\omega}$ is in A and the last number is in A^c, there exist consecutive numbers ν_{j_0-1}, ν_{j_0} such that $\nu_{j_0-1} \in A$ and $\nu_{j_0} \in A^c$; these can be taken to be, respectively, the numbers α and β of the lemma.

We now prove the previously stated theorem.

Proof. Since (1) holds trivially when either $A = \phi$ or $k = n$, we may assume that $A \neq \phi$ and $k < n$. Consider the set of ordered pairs,

$$E = \{(\alpha,\beta): \alpha \in A,\ \beta \text{ is an extension of } \alpha\}$$

Since each number $\alpha \in A$ has precisely $n-k$ extensions, $|E| = |A|(n-k)$. If we now set

$$F = \left\{ (\alpha,\beta) : \beta \in A^+,\ \alpha \text{ is a restriction of } \beta \right\},$$

it is clear that $E \subseteq F$ and $|F| = (k+1)|A^+|$. Hence,

$$(k+1)|A^+| \geqslant |A|(n-k),$$

which is equivalent to (1).

If $|A| = C(n,k)$, then

$$C(n,k+1) \geqslant |A^+| \geqslant C(n,k+1),$$

so that equality holds in (1).

Suppose conversely that $A \neq \phi$ and

$$|A^+| = \frac{|A|C(n,k+1)}{C(n,k)} = \frac{|A|(n-k)}{k+1}. \tag{2}$$

We wish to prove that $|A| = C(n,k)$; since this is trivial for the cases $k=0$ and $k=n$, we may restrict attention to integers k such that $0<k<n$. If $|A| < C(n,k)$, by the lemma there are numbers $\alpha \in A$, $\beta \in A^c \cap D_k$ such that α and β differ in exactly one factor. Let $\alpha = rp_1$ and $\beta = rp_2$, with $p_1 \neq p_2$, and put $\gamma = rp_1p_2$. Then $\gamma \in A^+$ and

$$(\beta,\gamma) \in E^c \cap F. \tag{3}$$

On the other hand, (2) implies that

$$|F| = (k+1)|A^+| = |A|(n-k) = |E|.$$

Since $E \subseteq F$, we conclude that $E = F$, which contradicts (3). Thus, $|A| = C(n,k)$.

Recently, it was communicated to the author that the second part of the theorem with m any integer and with $|D_k|$ in place of $C(n,k)$ is false. For example, if $m=12$, $k=1$, $A = \{3\}$, then $|D_k| = |D_{k+1}| = 2$, $A^+ = \{6\}$. Thus,

$$|A^+| = (|A|\,|D_{k+1}|)/\,|D_k| \qquad \text{and yet}$$

$A \neq D_k$. Nevertheless, it is the author's conjecture that the first part of the theorem remains true if one omits the hypothesis that m is a squarefree number and if one substitutes $|D_k|$ for $C(n,k)$. However, the above assertion has not been proved completely by the author.

REFERENCES

1. N.G. deBruijn, Ca. van Ebbenhorst Tengbergen and D. Kruysijk, "On the Set of Divisors of a Number," *Nieuw Arch. Wiskunde* (2) 23, (1951), pp. 191–193.
2. E. Sperner, "Ein Satz über Untermengen einer endlichen Menge," *Math. Z.,* 27 (1928), pp. 544–548.

****