ON A PROBLEM IN THE ELEMENTARY THEORY OF NUMBERS

By PAUL ERDÖS and PAUL TURÁN, Budapest, Hungary

1. The subject of this note is the following problem, proposed orally by G. Grünwald and D. Lázár. Let $p_1, p_2, \cdots, p_k$ be any prime numbers. We may say that N is *composed of* the primes $p_1, p_2, \cdots, p_k$ when every prime factor of N is one of these primes. Can we find an infinite set of different positive integers $a_1, a_2, \cdots$ so that every sum $a_i+a_j (i \neq j)$ is composed of $p_1, p_2, \cdots, p_k$? The answer that no such set exists was given by the proposers. Their proof depends on a theorem of Mr. Pólya asserting that if we denote by $q_1 < q_2 < \cdots < q_n < q_{n+1} < \cdots$ the numbers composed of the primes $p_1, p_2, \cdots, p_k$ then $q_{n+1} - q_n$ tends to infinity. But the proof of Pólya's theorem is not elementary; it seems therefore desirable to show the above result in an elementary way. On the other hand Pólya's theorem does not allow any further deductions in the following direction. Let $a_1, a_2, \cdots, a_n$ be a finite set of positive integers such that the sums a_i+a_j contain no prime factors other than $p_1, p_2, \cdots, p_k$; can we find an upper bound for the number n of such integers, depending on $p_1, p_2, \cdots, p_k$ or on k only? (Plainly we can suppose that $p_1 = 2$, because if the $p_1, p_2, \cdots, p_k$

are all odd, we find $n \leqq 2$. Indeed, otherwise at least one of a_1+a_2, a_1+a_3, a_2+a_3 would be even.)

We present an answer to the last question containing also the original problem. We show in an elementary way that $3 \cdot 2^{k-1}-1$ is an upper bound for n, i.e.

Theorem I. The two-term sums formed of $3 \cdot 2^{k-1}$ positive integers cannot all be composed of k given prime numbers.

From this we deduce as a corollary

Theorem II.

$$\pi(n) > \log_2\left(\frac{n}{3}\right)$$

where $\pi(n)$ denotes the number of primes $<n$.

The bound given in theorem I is probably not exact. The order of the maximum $n(k)$ of n belonging to a given number k of primes is probably[1]

$$n(k) = O(k^{1+\epsilon}) \text{ for any } \epsilon > 0$$

but actually we cannot prove this relation.

In the same way we may treat the analogous problem:

Is it possible to find two infinite sets of positive integers

$$a_1 < a_2 < \cdots$$
$$b_1 < b_2 < \cdots$$

so that every sum a_i+b_j shall be composed of the given primes $p_1, p_2, \cdots, p_k$? The answer is negative. The proof will show even more. We shall prove

Theorem III. The sums (a_i+b_j) formed of the two sets

$$a_1 < a_2 < \cdots < a_{k+1}$$
$$b_1 < b_2 < \cdots < b_\nu$$

cannot be composed of only k primes if one of the b's is greater than a_{k+1}^k. (This surely occurs if $\nu > a_{k+1}^k$.)

2. Before proving theorem I we shall prove the following

LEMMA: *Let $a_1 < a_2 < \cdots < a_n$ be a set of positive integers and $p>2$ a prime number. It is always possible to select out of this set at least[2] $\{n/2\} = N$ integers $a_{i_1}, a_{i_2}, \cdots, a_{i_N}$ with the following property: if a_{i_ν} is divisible exactly by p^{α_ν}, a_{i_μ} by p^{α_μ} and $a_{i_\nu}+a_{i_\mu}$ by $p^{\beta_{\mu\nu}}$, then*

---

[1] $f(x) = Og(x)$ means that there exists a B and an A such that for all $x \geqq B$ it is true that $|f(x)| < Ag(x)$; see Landau, *Primzahlen*, vol. 1, p. 31.

[2] The symbol $\{x\}$ denotes the smallest integer $\geqq x$.

$$\beta_{\mu\nu} = \min(\alpha_\mu, \alpha_\nu),$$

where $\min(\alpha_\mu, \alpha_\nu)$ *means the smaller of* α_μ *and* α_ν.

We divide every member of the set $a_1, a_2, \cdots, a_n$ by the highest possible power of p; thus we obtain the integers $a_1^1, a_2^1, \cdots, a_n^1$ (some of them being possibly equal). No member of this new set is divisible by p. We divide the members of this set into two classes according as their smallest positive residue, mod p, is less than or greater than $p/2$. At least one of these two classes must contain N of the a_ν^1. We retain only these; it is clear that the two-term sums formed of these are not divisible by p. The integers a corresponding to these a_ν^1 satisfy the requirement of our lemma. (The lemma is trivial except when some of the a's are divisible by the same power of p.)

3. We can now prove theorem I. Let $n=3\cdot 2^{k-1}$ and $a_1, a_2, \cdots, a_n$ be any positive integers. Suppose that all two-term sums of these are composed of k primes $p_1=2, p_2, \cdots, p_k$; we shall prove that this supposition leads to a contradiction.

We apply our lemma with $p=p_k$; we obtain then $3\cdot 2^{k-2}$ integers a_ν with the property in the lemma. Repeat the same process with $p=p_{k-1}$ upon this system of $3\cdot 2^{k-2}$ integers and so on. Finally we obtain three numbers a_1, a_2, a_3 of the same property with respect to the primes $p_2, p_3, \cdots, p_k$. Let

$$a_1 + a_2 = 2^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} \tag{1}$$

$$a_1 + a_3 = 2^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k} \tag{2}$$

$$a_2 + a_3 = 2^{\gamma_1} p_2^{\gamma_2} \cdots p_k^{\gamma_k}; \tag{3}$$

then a_1 and a_2 are divisible by $p_2^{\alpha_2}, \cdots, p_k^{\alpha_k}$; therefore a_1 and a_2 cannot be divided by 2^{α_1}. Hence by (1) a_1 and a_2 must contain the same power of 2. This evidently holds for a_1 and a_3 also. Let us denote this common exponent by γ. Then dividing (1), (2) and (3) by 2^γ, and denoting $a_i/2^\gamma$ by b_i we have

$$b_1 + b_2 = 2^{\delta} p_2^{\alpha_2} \cdots p_k^{\alpha_k} \tag{4}$$

$$b_1 + b_3 = 2^{\epsilon} p_2^{\beta_2} \cdots p_k^{\beta_k} \tag{5}$$

$$b_2 + b_3 = 2^{\theta} p_2^{\gamma_2} \cdots p_k^{\gamma_k}. \tag{6}$$

Here b_1, b_2 and b_3 are odd and each member of the left side of (4) (5) and (6) is divisible by the odd prime-powers on the respective right side. Dividing (4) by $p_1^{\alpha_1}, \cdots, p_{k-1}^{\alpha_{k-1}}$ we get a number >2, for the members on the left side are *different* odd numbers. By this $\delta \geqq 2$ and by analogous reasoning $\epsilon \geqq 2$ and $\theta \geqq 2$. Thus from (4), (5) and (6) it follows that the two-term sums formed of three different odd numbers are all divisible by 4, which is impossible.

4. In order to obtain the inequality of theorem II, let $a_\nu = \nu$ for $\nu = 1, 2, \cdots, \{n/2\}$. Then the prime divisors of the sums $a_i + a_j$ are the primes $\leqq n$. Hence by theorem I, $n/2 < 3\cdot 2^{\pi(n)-1}$, from which we immediately obtain the inequality stated in the introduction.

5. Finally we will prove our theorem III. Let

$$a_1 < a_2 < \cdots < a_{k+1},$$
$$b_1 < b_2 < \cdots < b_\nu$$

be given integers, $b_\nu > a_{k+1}^k$ and suppose that the sums $a_i + b_l$ are all composed of k prime factors $p_1, p_2, \cdots, p_k$. Let us consider the sums

$$a_1 + b_\nu,\ a_2 + b_\nu,\ \cdots,\ a_{k+1} + b_\nu.$$

We next show that one of these $a_l + b_\nu$ contains a power of one of the given primes, say $p_{i_l}^{\alpha_l}$, so that

$$p_{i_l}^{\alpha_l} > a_{k+1} \qquad (l = 1, 2, \cdots, k+1).$$

This we deduce from the fact that $a_l + b_\nu > b_\nu > a_{k+1}^k$ and that $(a_l + b_\nu)$ can have only k different prime factors. We call this prime p_{i_l} (or if there are several, any one of them) "the prime belonging to a_l." We assert that the primes belonging to different a_l are different. For if the same p should belong to a_{l_1} and a_{l_2}, then $(a_{l_1} - a_{l_2})$ would be divisible by p^m, where m is the smaller of α_{l_1} and α_{l_2}; but according to what has been said before, $p^m > a_{k+1}$, whereas both of the numbers a_{l_1} and a_{l_2} are positive and $< a_{k+1}$. Since the same prime can not belong to two integers, it is impossible that k primes shall belong to $(k+1)$ integers. Hence the supposition that all the sums $a_i + b_l$ are composed of the k primes must be false.