UNIVERSITAS COMENIANA
ACTA MATHEMATICA UNIVERSITATIS COMENIANAE
L—LI—1987

REMARKS ON SOME PROBLEMS IN THE ELEMENTARY THEORY OF NUMBERS

ANDRZEJ MĄKOWSKI, Warsaw

Abstract. Some problems in the elementary theory of numbers from the collections of Erdös—Graham and Guy are solved or commented. They concern the sum of divisors, powerful numbers, sums of squares and other topics.

The purpose of the present paper is to solve and to comment some problems stated in [1] and [3]. Problems will be quoted in italics and those from [3] followd by the number of section in which they occur.

(B11). *Are there three distinct numbers l, m, n such that* $l\sigma(l) = m\sigma(m) = n\sigma(n)$?

We show that from any system of s different Mersenne primes one can obtain s different numbers n with the same value of $n\sigma(n)$.

Denote by M_p the number $2^p - 1$. Let A be the product of s different Mersenne primes:

$$A = \prod_{i=1}^{s} M_{p_i} \text{ and } n_j = 2^{p_j - 1}A/M_{p_j} (1 \leqslant j \leqslant s).$$

Then $n_j\sigma(n_j) = 2^{p_j - 1}A/M_{p_j} \cdot M_{p_j} \prod_{i=1}^{s} 2^{p_i}/2^{p_j} = 2^{\Sigma p_i - 1}A$,

which is independent of j.

This argument is a simple generalization of observation of Guy concerning the case $s = 2$.

(B16). *Erdös denotes by* $u_1^{(k)} < u_2^{(k)} < \ldots$ *the integers all of whose prime factors have exponents* $\geqslant k$. *He asks if the equation* $u_{i+1}^{(2)} - u_i^{(2)} = 1$ *has infinitely many solutions which do not come from Pell equations* $x^2 - dy^2 = \pm 1$. *What is the largest r such that there are* $u_{i_1}^{(2)}, \ldots, u_{i_r}^{(2)}$ *in arithmetic progression? Are there infinitely many such r-tuples? Erdös conjectures that there are infinitely many triples of* $u_i^{(3)}$ *in arithmetic progression, but no quadruples, and no triples of* $u_i^{(4)}$. *Also that* $u_i^{(3)} + u_j^{(3)} = u_k^{(3)}$ *has infinitely many solutions, but that* $u_i^{(4)} + u_j^{(4)} = u_k^{(4)}$

has at most a finite number. More generally that the sum of $k - 2$ *of the* $u_i^{(k)}$ *is at most finitely many cases equal to* $u_i^{(k)}$.

Let $U^{(k)} = (u_n^{(k)})_{n=1}^{\infty}$.

The equation $7^3x^2 - 3^3y^2 = 1$ has a solution $\langle x, y \rangle = \langle 376\,766, 1\,342\,879 \rangle$. From the theory of quadratic equation with two unknowns (cf. [5], p. 57) it follows that it has infinitely many solutions in positive integers x, y. The numbers 3^3y^2 and 7^3x^2 are terms of $U^{(2)}$ difering by 1 (hence consecutive) and both are not squares. Therefore the answer to the first question is in the affirmative.

We observe that the numbers $(2^{k+1} - 1)^k$, $2^k(2^{k+1} - 1)^k$ and $(2^{k+1} - 1)^{k+1}$ are in A. P. and belong to $U^{(k)}$. Assume that $a_1, a_2, \ldots, a_s$ are s consecutive terms of A. P. with difference d, which belong to $U^{(k)}$. Then $a_1(a_s + d)^k, a_2(a_s + d)^k, \ldots, a_s(a_s + d)^k$, $(a_s + d)^{k+1}$ form A.P. consisting of $s + 1$ terms belonging to $U^{(k)}$. Thus there exist arbitrarily long finite arithmetic progressions consisting of different terms of $U^{(k)}$.

We have identity

$$a^k(a^l + a^{l-1} + \ldots + a + 1)^k + a^{k+1}(a^l + l^{l-1} + \ldots + a + 1)^k +$$

$$+ \ldots + a^{k+1}(a^l + a^{l-1} + \ldots + a + 1)^k = a^k(a^l + a^{l-1} + \ldots + a + 1)^{k+1}.$$

Hence $u_{i_1}^{(k)} + u_{i_2}^{(u)} + \ldots + u_{i_{l+1}}^{(k)} = u_m^{(k)}$ has infinitely many solutions for every k and l.

Problems on arithmetic progressions and sums of terms of $U^{(k)}$ become difficult when we require that the considered numbers are relatively prime.

(B48)*David Silverman noticed that if* p_n *is the* n^{th} *prime, then*

$$\prod_{n=1}^{m} \frac{p_n + 1}{p_n - 1}$$

is an integer for $m = 1, 2, 3, 4$ *and* 8, *and asked whether it is ever again an integer.*

This problem can be generalized as follows: Determine positive integers n for which $\sigma(n)$ is divisible by $\varphi(n)$, where φ is the Euler totient function and σ — the sum of divisors. Then the problem of Silverman concerns the numbers

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

We observe that

$$\sigma(n) = 4\varphi(n) \tag{1}$$

if $2n$ is a perfect number greater than 6.

In fact, we have $n = 2^{p-2}(2^p - 1)$, where $2^p - 1$ is a prime number and $p \geqslant 3$ (cf. [2], p. 240), hence $\sigma(n) = (2^{p-1} - 1) \cdot 2^p = 4 \cdot 2^{p-3}(2^p - 2 = 4\varphi(n)$. Unfortunately, the converse is not true as (1) is satisfied for example by $3 \cdot 5 \cdot 7$, $2 \cdot 11 \cdot 19$, $3 \cdot 5 \cdot 11 \cdot 19$, $3 \cdot 7 \cdot 11 \cdot 17 \cdot 19$, $3 \cdot 7 \cdot 11 \cdot 13 \cdot 29$.

However, if n is even and satisfies (1), then $2n$ is either perfect or abundant (i.e. $\sigma(2n) \geqslant 4n$).

To prove this we put $n = 2^{r-1}m$, where $r \geqslant 2$, m odd. Then

$$\sigma(n) = (2^r - 1)\sigma(m),\ \sigma(2n) = \sigma(2^r m) = (2^{r+1} - 1)\sigma(m) =$$
$$= 2^r\sigma(m) + (2^r - 1)\sigma(m) = 2^r\sigma(m) + \sigma(n) = 2^r\sigma(m) + 4\varphi(n) =$$
$$= 2^r\sigma(m) + 4\varphi(2^{r-1}m) = 2^r\sigma(m) + 4 \cdot 2^{r-2}\varphi(m) =$$
$$= 2^r(\sigma(m) + \varphi(m)) \geqslant 2^{r+1}m = 4n\,.$$

The last inequality follows from the inequality $\sigma(m) + \varphi(m) \geqslant 2m$ (cf. [4]), whore equality holds only for m equal to 1 or a prime number.

Therefore, as (1) is not satisfied by $n = 2^s$, we may assert that an even number $n = 2^{r-1}m$ (m odd) satisfying (1) is a half of a perfect number if and only if m is a prime number.

If $n = 2^{p-2}m$ ($p \geqslant 3$, m odd) satisfies (1) and m is prime, them $m = 2^p - 1$. This follows from the equality $(2^{p-1} - 1)(m + 1) = 4 \cdot 2^{p-3}(m - 1)$.

If n is odd and satisfies (1), then $2n$ is abudant. For, $\sigma(2n) = 3\sigma(n) = 2\sigma(n) + 4\varphi(n) > 2(\sigma(n) + \varphi(n)) \geqslant 4n$. The above arguments show also that the inequality $\sigma(n) > 4\varphi(n)$ implies that $2n$ is abundant.

If for some integer a we have $\sigma(n) = a\varphi(n)$ and for some prime number p not dividing n the number $b = a\dfrac{p+1}{p-1} = a + \dfrac{2a}{p-1}$ is integer, then $\sigma(np) = b\varphi(np)$. In particular, if $3 \nmid n$ and $\varphi(n) | \sigma(n)$, then $\varphi(3n) | \sigma(3n)$.

(C 20) *Paul Turán conjectures that all positive integers can be represented as the sum of at most five pairwise coprime squares. Are all sufficiently large integers representable as the sum of exactly five pairwise coprime squares?*

From consideration modulo 3 of the equation $3k = x_1^2 + x_2^2 + x_3^2 + x_4^2 + x_5^2$ it follows that for some i, j such that $1 \leqslant i < j \leqslant 5$ we have $3 | x_i$, $3 | x_j$. Hence the answer to the last question is in the negative.

To disprove Trán's conjecture consider the numbers $n = 2^{2k} \cdot 3 \cdot (8m + 5)$ with $k \geqslant 2$. We have $n = 4^k[8(3m + 1) + 7]$, hence n is not the sum of less than four squares. Since these numbers are divisible by 3, they are not the sums of five coprime squares. From consideration modulo 8 it follows that n is not the sum of four coprime squares.

(F 10) *The Lehmers have shown that the smallest solution of* $2^n \equiv 3 \pmod{n}$ is $n = 4\,700\,063\,497 = 19 \cdot 47 \cdot 5\,263\,229$. *Of course n has to be composite, and it is not divisible by any of* 2, 3, 7, 17, 31, 41, 43, 73, ... *What are these primes?*

We show that no prime p of the from $24k \pm 7$ and $24k \pm 11$ is a divisor of n satisfying $2^n \equiv 3 \pmod n$. In fact, n is odd: $n = 2k+1$. Hence $2^{2k+1} \equiv 3 \pmod p$ and $\left(\frac{2}{p}\right) = \left(\frac{3}{p}\right)$. Let $\varepsilon \in \{+1, -1\}$. We have $\left(\frac{\varepsilon}{3}\right) = \varepsilon$, $(-1)^{\frac{1}{2}(\varepsilon+1)} = -\varepsilon$ and $\frac{1}{2} \cdot$ $\cdot (34k + 9\varepsilon \pm 2\varepsilon - 1) \equiv \frac{1}{2}(\varepsilon + 1) \pmod 2$. For prime number $p = 24k +$ $+ 9\varepsilon \pm 2\varepsilon$ we have (we consider either lower or upper sings) $\left(\frac{3}{p}\right) = (-1)^{\frac{1}{2}(p-1)} \cdot$

$$\cdot \left(\frac{p}{3}\right) = (-1)^{\frac{1}{2}(\varepsilon+1)}\left(\frac{24k + 9\varepsilon \pm 2\varepsilon}{3}\right) = -\varepsilon\left(\frac{\pm 2\varepsilon}{3}\right) = -\varepsilon\left(\frac{\pm \varepsilon}{3}\right) = -\varepsilon(\mp \varepsilon) =$$

$$= \pm 1 = -\left(\frac{2}{p}\right), \text{ a contradiction.}$$

([3], **p. 88**) *Let m and n be positive integers and consider the two sets $\left\{k(m-k) \colon 1 \leqslant k \leqslant \frac{m}{2}\right\}$ and $\left\{l(n-1) \colon 1 \leqslant l \leqslant \frac{n}{2}\right\}$. Can one estimate the number of integers common to both? Is this number unbounded? It should certainly be less than $(mn)^\varepsilon$ for every $\varepsilon > 9$ if mn is sufficiently large.*

We show below that the answer to the second question is in the affirmative.

Let $f(m, n)$ be the number of integers common to the sets defined in the problem and $d(k)$ — the number of divisors of k. We show that

$$f(2(a-1), 2(a+1)) \geqslant \frac{1}{2} d(a). \tag{2}$$

Let $a = A_1 A_2$ be any representation of a as the product of two factors $(A_1 \leqslant A_2)$. Evidently there are at least $\frac{1}{2} d(a)$ such representations. Each of them determines a common element of the two sets constructed for $m = 2(a-1)$ and $n = 2(a+1)$. This element is equal to $(A_1^2 - 1)(A_2^2 - 1)$. In fact, we have $(A_1 + 1)(A_2 - 2) + (A_1 - 1)(A_2 + 1) = 2(a - 1)$, $(A_1 + 1)(A_2 + 1) + (A_1 - 1)(A_2 -) = 2(a + 1)$, $(A_1 + 1)(A_2 - 1) \cdot (A_1 - 1)(A_2 + 1) = (A_1^2 - 1)(A_2^2 - 1] = (A_1 + 1)(A_2 + 1) \cdot (A_1 - 1)(A_2 - 1)$. Further, the numbers $(A_1^2 - 1)(A_2^2 - 1)$ corresponding to different representations $a = A_1 A_2$ are different. Suppose that $(A_1^2 - 1)(A_2^2 - 1) = (B_1^2 - 1)(B_2^2 - 1)$, $a = A_1 A_2 = B_1 B_2$. Then $A_1^2 + A_2^2 = B_1^2 + B_2^2$, $A_1 A_2 = B_1 B_2$, $(A_1 + A_2)^2 = (B_1 + B_2)^2$, $A_1 + A_2 = B_1 + B_2$.

The sum and product of two numbers determine them. The proof of (2) is completedd.

For $a = p_1 p_2 \ldots p_r > a_0(\varepsilon)$ (a is the product of consecutive primes) we have the inequality

$$\log d(a) > \frac{(1-\varepsilon)\log a \log 2}{\log\log a}$$

(cf. [2], p. 263). For such a we obtain

$$f(2(a-1), 2(a+1)) > \frac{1}{2} a^{\frac{(1-\varepsilon)\log 2}{\log\log a}}.$$

REFERENCES

1. Erdös, P.—Graham, R. L.: Old and new problems and results in combinatorial number theory, Genève, Universite de Genève 1980.
2. Hardy, G. H.—Wright, E. M.: An introduction to the theory of numbers, 5th edition, Oxford, Oxford University Press 1979.
3. Guy, R. K.: Unsolved problems in number theory, New York — Heidelberg — Berlin, Springer — Verlag 1981.
4. Mąkowski, A.—Schinzel, A.: Aufgabe 339. Elem. Math. (1960) 15, 39—40.
5. Mordell, L. J.: Diophantine equations, London — New York, Academic Press 1969.

Author's address: Received: 14. 9. 1985
Andrzej Mąkowski
Institute of Mahtematics
University of Warsaw
PL 00-901 Warsaw PKiN

РЕЗЮМЕ

ЗАМЕЧАНИЯ О НЕКОТОРЫХ ПРОБЛЕМАХ ЭЛЕМЕНТАРНОЙ ТЕОРИИ ЧИСЕЛ

Андржей Монковски, Варшава

Приводятся решения или комментарии к нескольким проблемам элементарной теории чисел, поставленным в книгах Эрдёша—Грэхема и Гая. Эти проблеммы касаются суммы делителей чисел, являющихся произведениями степеней простых чисел, суммы квадратов и других вопросов.

SÚHRN

POZNÁMKY K NIEKTORÝM
PROBLÉMOM Z ELEMENTÁRNEJ TEÓRIE CÍSEL

Andrzej Makowski, Varšava

V práci sú uvedené riešenia alebo poznámky k niektorým problemom z knihy Erdösa a Grahama a z knihy od Gaya. Uvedené problémy sa dotýkajú sumy deliteľov, sumy štvorcov čísel, ktorých prvočíselné delitele majú exponenty väčšie ako zadané číslo atď.