Štefan Porubský; Kazimierz Szymiczek

The 3rd Czech and Polish Conference on Number Theory. Problem session

Acta Mathematica et Informatica Universitatis Ostraviensis, Vol. 8 (2000), No. 1, 7--10

Persistent URL: `http://dml.cz/dmlcz/120552`

The 3rd Czech and Polish Conference on Number Theory

Ostravice, June 13–16, 2000

Problem session

The Problem Session, chaired by Andrzej Schinzel, took place on June 16, 2000. The following twelve problems were proposed.

1. A. Rotkiewicz:
Given integers L, M with $K = L - 4M$ not a square. Do there exist infinitely many arithmetic progressions formed by three distinct Lehmer pseudoprimes with parameters L and M?

2. A. Rotkiewicz:
Given integers L, M with $K = L - 4M$ not a square and $\varepsilon = \pm 1$. Do there exist infinitely many, or at least one, arithmetic progressions formed by three distinct Lehmer pseudoprimes with parameters L and M satisfying $(KL/M) = \varepsilon$, where (KL/M) is the Jacobi symbol?

A. Rotkiewicz, *Arithmetic progressions formed by pseudoprimes*, Acta Math. et Inform. Univ. Ostrav. 8 (2000)

3. M. Paštéka:
I. Niven proved in 1951 the following result. Let A be a subset of the set $\mathbb{N}$ of positive integers, p a prime and $A_p = \{a \in A \ : \ p \mid a, p^2 \nmid a\}$. If P is a set of primes with $\sum_{p\in P} p^{-1}$ diverging and such that for every $p \in P$ the set A_p has vanishing asymptotic density, then the asymptotic density of A also vanishes. Let $\mathcal{D}$ be the class of all sequences of positive integers possessing asymptotic density, that is, $A \in \mathcal{D}$ if and only if there exists the limit $\lim_{n\to\infty} A(n)/n$, where $A(n)$ is the counting function for the set A, i.e., $A(n) = \#\{a \in A : a \le n\}$.

Prove or disprove: $A \in \mathcal{D}$ if and only if there exists a set of primes P with $\sum_{p\in P} p^{-1}$ diverging such that $A_p \in \mathcal{D}$ for every $p \in P$.

Collected and edited by Š. Porubský and K. Szymiczek

I. NIVEN, *The asymptotic density of sequences*, Bull. Amer. Math. Soc. **57** (1951), 420–434 (Corollary 1, p. 426).

I. NIVEN, H. S. ZUCKERMAN, *An Introduction to the Theory of Numbers* (3rd ed.), J. Wiley & Sons, New York – London – Sydney – Toronto 1972 (11.7. Theorem).

4. M. Paštéka:

We write $A \bigodot B = \mathbb{N}$ if for each $n \in \mathbb{N}$ there are $a \in A$ and $b \in B$ with $n = ab$. In 1976 P.Erdős and B. Saffari proved: If $A \bigodot B = \mathbb{N}$ then both A and B have asymptotic density and $\mathrm{d}(A) = \left(\sum_{b\in B} b^{-1}\right)^{-1}$. Find a characterization of all the direct factors of $\mathbb{N}$.

B. SAFFARI, *On the asymptotic density of sets of integers.* J.-London-Math.-Soc. (2) **13** (1976), no. 3, 475–485. *Existence de la densite asymptotique pour les factuers directs de* $\mathbf{N}^*$. C. R. Acad. Sci. Paris Ser. A-B **282** (1976), no. 5, Ai, A255–A258.

5. G. Banaszak:

Disprove the following statement. Let a, b, c, d be positive integers such that $a > 1$, $c > 1$ and $a \neq c$. There exists a p_0 such that for all primes $p > p_0$ and all positive integers n

$$a^n \equiv b \pmod p \quad \Leftrightarrow \quad c^n \equiv d \pmod p.$$

This has been resolved in the following cases:

- $b = d = 1$ (C. Corralez–Rodrigáñez and R. Schoof),
- $a = d = 2$, $b = c = 3$ and $a = d = 2$, $b = c = 5$ (G. Banaszak),
- $a = d = 2^{m_0} p_1^{2m_1} p_2^{2m_2} \ldots p_r^{2m_r}$, $b = c = p_{r+1}$, where $p_1 < p_2 < \ldots$ is the sequence of consecutive odd primes, m_0 is an odd positive integer, $m_1, \ldots, m_r$ are arbitrary positive integers and r is such that $p_{r+1} \equiv 3$ or $5 \pmod 8$ (G. Banaszak).

G. BANASZAK, Mod *p logarithms* $\log_2 3$ *and* $\log_3 2$ *differ for infinitely many primes*, Ann. Math. Sil. **12** (1998), 141–148.

C. CORRALEZ–RODRIGÁÑEZ, R. SCHOOF, *Support problem and its elliptic analogue*, J. Number Theory **64** (1997), 276–290.

6. K. Szymiczek:

Let a and b be natural numbers. A prime p is said to be an (a, b)–divisor if there exists a natural number n such that

$$p \mid a^n - b \qquad \text{and} \qquad p \mid b^n - a.$$

Using GP/Pari calculator we have found in 450 hours of computer work the following results: For $a, b \in \{2, 3, 5, 7\}$ and $n \le 50\,000$ only the following primes occur as (a, b)–divisors

- $(2,3)$–divisors: 5, 5: 333
- $(2,5)$–divisors: 3, 1: 031, 1: 409
- $(2,7)$–divisors: 5, 13, 61, 67, 211, 19: 423
- $(3,5)$–divisors: 2, 7, 2: 333, 8: 537, 13: 757, 37: 123

- $(3,7)$–divisors: 2, 5, 79, 300: 673
- $(5,7)$–divisors: 2, 17, 97, 227: 251

Prove that for all $a, b \in \mathbb{N}$ there are infinitely many (a,b)–divisors.

K. SZYMICZEK, *On the common factors of* $2^n - 3$ *and* $3^n - 2$. Functiones et Approximatio, to appear.

7. K. Szymiczek:

For a prime number p and a natural number a not divisible by p let $\ell_p(a)$ be the order of a modulo p. Using GP/Pari calculator we have found that there are only two prime numbers less than 10 000 000 with the property that the numbers 2 and 3 have relatively prime orders modulo p. These are

$$p = 683, \qquad \ell_p(2) = 22, \qquad \ell_p(3) = 31$$
$$p = 599\,479, \qquad \ell_p(2) = 33, \qquad \ell_p(3) = 18\,166.$$

Question: Do there exist infinitely many primes p satisfying

$$\gcd(\ell_p(2), \ell_p(3)) = 1\ ?$$

8. C. Greither:

Find an algorithm for calculating the minus class group of an Abelian field, nearly as efficient as the standard algorithm for the minus class number via Stickelberger elements.

9. W. Narkiewicz:

Let $N > 3$ be an integer. Prove (or disprove) that for every prime $p \geq p_0(N)$ there exists a quadratic polynomial over $GF(p)$, having a cycle of length N in that field.

10. W. Gajda:

Let ℓ be a fixed odd prime, n a fixed even positive integer. For every $k \geq 1$ put

$$\xi_{\ell^k} = e^{2\pi i/\ell^k}, \qquad u_k = \prod_{\substack{1 \leq a < e^k \\ (a,\ell)=1}} (1 - \xi_{\ell^k}^a)^{a^n}, \qquad A_k = N(u_k - 1),$$

where $N(\cdot)$ denotes the norm down to $\mathbb{Q}$.

1. [(a)] Calculate A_k, or
2. [(b)] Find the rate of growth of A_k for $k \to \infty$.

11. A. Schinzel:

Consider the linear equation $\sum_{i=0}^{k} a_i x_i = 0, \quad a_i \in \mathbb{Z}$. By Siegel's lemma there exists a nonzero solution $\mathbf{x} = (x_0, \ldots, x_k)$ in $\mathbb{Z}^{k+1}$ such that

$$h(\mathbf{x}) := \max |x_i| \leq \big(c(k) \max |a_i|\big)^{\frac{1}{k}}.$$

For

$$c_0(k) = \sup_{\mathbf{a}\in\mathbb{Z}^{k+1}\setminus\{0\}} \inf_{\substack{\mathbf{x}\in\mathbb{Z}^{k+1}\setminus\{0\}\\ \mathbf{a}\cdot\mathbf{x}=0}} \frac{h(\mathbf{x})^k}{h(\mathbf{a})}$$

it is known that

$$c_0(1) = 1, \qquad c_0(2) = \frac{4}{3}, \qquad c_0(3) = \frac{27}{19}, \qquad c_0(k) \le \sqrt{k+1}.$$

Find $c_0(4)$ or at least some bounds.

E. Bombieri and J. D. Vaaler, *On Siegel's lemma*, Invent. Math. **73** (1983), 11-32. Addendum, ibid. **73** (1984), 377.

S. Chaładus and A. Schinzel, *A decomposition of integer vectors II*, Pliska Stud. Mat. Bulgar. **11** (1991), 15–23.

S. Chaładus, *On the densest lattice packing of centrally symmetric octahedra*, Math. Comp. **58** (1992), 341–345.

12. A. Schinzel:

(Arising from the work of W. M. Schmidt.) Consider a polynomial

$$f(x) = \sum_{i=0}^{n} a_i x^i$$

with nonnegative coefficients a_i and such that the polynomial

$$f(x)^2 = \sum_{i=0}^{2n} b_i x^i$$

has all coefficients $b_i \le 1$. Let

$$S(n) = \sup \sum_{i=0}^{2n} b_i = \sup f(1)^2,$$

the supremum over all polynomials satisfying the above conditions. Schmidt has shown that $S(n) \sim cn$ as $n \to \infty$ with the constant c satisfying $\frac{4}{\pi} \le c < 2$. This has been improved by A. Schinzel to $\frac{4}{\pi} \le c \le \frac{7}{4}$. Determine the value of c or at least improve the bounds.