Nonlinear Analysis: Modelling and Control, Vilnius, IMI, 1999, No 4, pp. 23-30

# ON WARING'S PROBLEM FOR A PRIME MODULUS

**A. Dubickas**
Department of Mathematics and Informatics, Vilnius University, Naugarduko 24, LT-2006 Vilnius, Lithuania
e-mail: *arturas.dubickas@maf.vu.lt*

Abstract

We obtain a lower bound for the minimum over positive integers such that the sum of certain powers of some integers is divisible by a prime number, but none of these integers is divisible by this prime number.

**Keywords:** Waring's problem modulo prime number.

Let $k \geqslant 2$ be a positive integer and let $p$ be a prime number. We put $\gamma(k,p)$ for the smallest $\gamma$ such that for any integer $x$ the congruence

$$x \equiv x_1^k + x_2^k + \ldots + x_\gamma^k (\bmod p)$$

is solvable in integers $x_1, x_2, \ldots, x_\gamma$. The problem of finding $\gamma(k,p)$ is called *Waring's problem modulo p*. Let also $\theta(k,p)$ be the smallest $\theta$ such that the congruence

$$x_1^k + x_2^k + \ldots + x_\theta^k \equiv 0 (\bmod p)$$

has a nontrivial solution, i.e. not all $x_j$ are divisible by $p$.

Notice firstly that substituting $x = -1$ into the first congruence we obtain

$$\theta(k,p) \leqslant \gamma(k,p) + 1. \tag{1}$$

Secondly, if $d$ is the greatest common divisor of $k$ and $p-1$ then $\gamma(k,p) = \gamma(d,p)$ and $\theta(k,p) = \theta(d,p)$. Therefore, without loss of generality we can assume that $p \equiv 1 (\bmod k)$.

In 1927, G. H. Hardy and J. E. Littlewood [8] proved that

$$\gamma(k,p) \leqslant k. \tag{2}$$

For $p = k+1$ we have $\gamma(k,p) = k$, so that the inequality (2) cannot be improved in general. However, if $p$ is large compared to $k$ the upper bound (2) can be strengthened. In 1971, M. M. Dodson [5] showed that $\gamma(k,p) < c_1 \log k$ if $p > k^2$ (here and below $c_1, c_2, \ldots$ are some positive constants). Various improvements of (2) were also obtained by M. M. Dodson and A. Tietäväinen [6], J. D. Bovey [1], A. Garsia and J. F. Voloch [7]. By (1) all these results imply that the inequality

$$\theta(k,p) \leqslant k+1 \tag{3}$$

can be strengthened for $p > k+1$. The inequalities better that (3) were obtained by S. Chowla, H. B. Mann and E. G. Straus [3], I. Chowla [2]. In 1975, A. Tietäväinen [12] proved that $\theta(k,p) \leqslant c_2(\varepsilon) k^{1/2+\varepsilon}$ for $p > k+1$.

Using E. Dobrowolski's work on Lehmer's conjecture [4] S. V. Konyagin [10] obtained new estimate for Gaussian sums which implies new upper bounds for $\gamma(k,p)$ and $\theta(k,p)$. In particular, he proved [10, Theorem 3] the inequality

$$\theta(k,p) \leqslant c_3(\varepsilon)(\log k)^{2+\varepsilon}$$

for $p > k+1$ which gives an affirmative answer to Heilbronn's question [9]. Moreover, he conjectured that a stronger inequality $\theta(k,p) \leqslant c_4 \log k$ holds and gave lower bounds on $\gamma(k,p)$ [10, Theorem 4] and $\theta(k,p)$ [10, Theorem 5] for an infinite set of values $k$ and $p$.

Our principal objective in this paper is to illustrate some of the techniques used in the proof of [10, Theorem 5] and at the same time make a contribution to the subject by improving slightly the lower bound on $\theta(k,p)$ and giving more precise information on primes $p$ for which this lower bound holds.

Suppose $f : \mathbb{N} \to [1;\infty)$ is a nondecreasing function. Let $k$ be a sufficiently large positive integer. We will consider three cases:

i) $f(k) \leqslant \log k / 2\log\log k$,

ii) $\log k/2\log\log k < f(k) < 2\log k$,

iii) $2\log k \leqslant f(k) \leqslant (\log k)^A$ for some $A > 1$.

Theorem. *Let $\varepsilon > 0$. There exist infinitely many positive integers $k$ and primes $p$ such that $p \equiv 1 (\mathrm{mod}\, k)$,*

$$k \max\left\{ f(k); \frac{\log k}{2\log\log k} \right\} \leqslant p \leqslant (1+\varepsilon)k \max\left\{ f(k); \frac{\log k}{2\log\log k} \right\}$$

*and*

*1) $\theta(k,p) > \log k/2\log\log k$ in case i),*

*2) $\theta(k,p) > f(k)/6$ in case ii),*

*3) $\theta(k,p) > \log k / 5 \log\big(f(k)/\log k\big)$ in case iii).*

REMARK. *Taking, e. g.,* $f(k) = (\log k)^A$ *with* $A > 1$ *(case iii)) we obtain*

$$\theta(k,p) > \frac{\log k}{5(A-1)\log\log k},$$

*whereas* [10, Theorem 5] *gives* $\theta(k,p) > (\log k)^{1-\varepsilon}$.

*Note that by (1) the lower bounds for* $\theta(k,p)$ *imply the lower bounds for* $\gamma(k,p)$ *of the same shape.*

*Proof of the theorem.* Let us fix a number $\varrho > 1$ and let $f(x) = f([x])$ for $x \in [1;\infty)$. We will show first that there exist infinitely many $s \in \mathbb{N}$ such that $f(\varrho s) < \varrho f(s)$. This will allow us to replace the function of the form $f(k) = (\log k)^A$ used in [10] by an arbitrary nondecreasing function satisfying i), ii) or iii). Indeed, suppose that $f(\varrho s) \geqslant \varrho f(s)$ for all $s \geqslant s_0$. Then

$$1 \leqslant f(s_0) \leqslant \frac{1}{\varrho} f(\varrho s_0) \leqslant \ldots \leqslant \frac{1}{\varrho^m} f(\varrho^m s_0) \leqslant \frac{\left(\log \varrho^m s_0\right)^A}{\varrho^m} < \frac{1}{2}$$

for all sufficiently large $m$, a contradiction.

Let $s$ be one of these. We will show that there is an integer $k$, $s \leqslant k \leqslant \varrho s$, for which the statement of the theorem holds. Suppose $t$ is a smallest prime greater or equal than $\max\left\{\varrho f(\varrho s); \varrho \log(\varrho s)/2\log\log(\varrho s)\right\}$.

Now we will estimate the number of primes in the arithmetic progression

$$A(s,t,\varrho) = \{st+1, (s+1)t+1, \ldots, [\varrho s]t+1\}.$$

Suppose $p = kt+1$ is a prime in $A(s,t,\varrho)$ and let $\alpha$ be a primitive root modulo $p$. Put $\beta = \alpha^k$. Clearly, $\beta^t \equiv (\operatorname{mod} p)$ and each number $x^k$ modulo $p$ is congruent to one of the numbers $0, 1, \beta, \beta^2, \ldots, \beta^{t-1}$. If $\theta(k,p) \leqslant \theta_0$, there is a set of nonnegative integers $l_0, l_1, \ldots, l_{t-1}$ such that

$$0 < l_0 + l_1 + \ldots + l_{t-1} \leqslant \theta_0 \tag{4}$$

and

$$\sum_{j=0}^{t-1} l_j \beta^j \equiv 0 (\operatorname{mod} p). \tag{5}$$

Let

$$P(z) = \sum_{j=0}^{t-1} l_j z^j$$

be a polynomial corresponding to a fixed set $l_0, l_1, \ldots, l_{t-1}$. Consider the resultant of $P(z)$ and $Q(z) = 1 + z + \ldots + z^{t-1}$. If $\theta_0$ is equal to the right hand side of 1),

2) or 3), then $\theta_0 < t$. Combining this with the fact that $Q(z)$ is irreducible we get that $\mathrm{Res}(P,Q)$ is a nonzero integer. By Hadamard's inequality

$$|\mathrm{Res}(P,Q)| \leqslant \theta_0^t t^{t/2} < t^{3t/2}.$$

On the other hand, let $p$ be a prime in $A(s,t,p)$ for which the inequality opposite to 1), 2) or 3) holds and let $\beta$ be a respective power of a primitive root. Then for at least one of the sets satisfying (4) we have $P(\beta) \equiv 0 (\bmod p)$ (see (5)) and $Q(\beta) \equiv 0 (\bmod p)$. Thus, $p$ divides $\mathrm{Res}(P,Q)$ for at least one of the polynomials $P(z)$. Suppose there are $r$ such distinct primes which divide $|\mathrm{Res}(P,Q)|$. Then

$$(st+1)^r < t^{3t/2},$$

and

$$r < \frac{3t \log t}{2 \log s} \leqslant \frac{3t \log t}{2 \log(k/\varrho)}. \tag{6}$$

In case i) we have

$$\frac{\varrho \log k}{2 \log \log k} \leqslant t < \frac{\varrho^2 \log k}{2 \log \log k},$$

so that $r < 3\varrho^3/4 < 1$ if $\varrho$ is sufficiently close to 1. This shows that for all primes in $A(s,t,\varrho)$ the inequality 1) holds. The smallest prime in $A(s,t,\varrho)$ is greater than

$$st \geqslant kt/\varrho \geqslant k \log k / 2 \log \log k$$

and smaller than

$$\varrho^2 st \leqslant \varrho^2 kt < \varrho^4 k \log k / 2 \log \log k.$$

This completes the proof of 1), since in case i) we have

$$\max\left\{ f(k); \frac{\log k}{2 \log \log k} \right\} = \frac{\log k}{2 \log \log k}.$$

In cases ii) and iii) the number of sets satisfying (4) is equal to

$$\sum_{j=1}^{\theta_0} \binom{j+t-1}{t-1}.$$

By Stirling's formula, this does not exceed

$$\theta_0 \binom{\theta_0 + t}{t} < c_5 \theta_0 \Big(1 + \frac{\theta_0}{t}\Big)^t \Big(1 + \frac{t}{\theta_0}\Big)^{\theta_0} < c_5 \theta_0 \exp\Big(\theta_0 \log\big(e(1 + t/\theta_0)\big)\Big).$$

Hence, the number of primes in $A(s,t,\varrho)$ for which the inequality opposite to 2) (or 3)) holds is less than (see (6))

$$\frac{3t\log t}{2\log(k/\varrho)}\sum_{j=1}^{\theta_0}\binom{j+t-1}{t-1} < t^3\exp\Big(\theta_0\log\big(e(1+t/\theta_0)\big)\Big). \tag{7}$$

In case 2) $\theta_0 = f(k)/6$,

$$t < \varrho^2 f(\varrho s) < \varrho^3 f(s) \leqslant \varrho^3 f(k) < 2\varrho^3\log k,$$

so that (7) is less than $k^{0.99}$.

In case 3) $\theta_0 = \log k/5\log\big(f(k)/\log k\big)$,

$$t < \varrho^3 f(k) < \varrho^3(\log k)^A,$$

so that (7) is less than

$$\varrho^9(\log k)^{3A}\exp\left(\frac{\log k\big(1+\log\big(1+5\varrho^3\big(f(k)/\log k\big)\log\big(f(k)/\log k\big)\big)}{5\log\big(f(k)/\log k\big)}\right).$$

Since $f(k)/\log k \geqslant 2$, this expression is less than $k^{0.9}$. In both cases 2) and 3) we see that the number of primes in $A(s,t,\varrho)$ for which the inequality opposite to 2) (or 3)) holds is less than $k^{0.99}$.

By the asymptotic distribution law for primes in arithmetic progressions [11, Theorem 8.3] the set $A(s,t,\varrho)$ contains at least

$$(1-\delta)\frac{\varrho st}{\varphi(t)\log(\varrho st)} - (1+\delta)\frac{st}{\varphi(t)\log(st)} \tag{8}$$

primes for a given $\delta > 0$ and sufficiently large $s$. Since $\varphi(t) = t-1$ and

$$t < \varrho^2 f(\varrho s) < (\log s)^{A+1},$$

(8) is greater than

$$\frac{s}{(\log s)^2} > k^{0.991}.$$

This proves 2) and 3), since the smallest prime in $A(s,t,\varrho)$ is greater than

$$st \geqslant k(f(\varrho s) \geqslant k\, f(k)$$

and smaller than

$$\varrho^2 st \leqslant \varrho^2 kt < \varrho^4 k f(\varrho s) < \varrho^5 k\, f(k).$$

## ACKNOWLEDGEMENTS

This work was partially supported by Lithuanian State Studies and Science Foundation.

## REFERENCES

1. J. D. Bovey, A new upper bound for Waring's problem (mod $p$), *Acta Arith.* **32** (1977), pp. 157–162.

2. I. Chowla, On Waring's problem (mod $p$), *Proc. Ind. Nat. Acad. Sci. India Sect. A* **13** (1943), pp. 195–200.

3. S. Chowla, H. B. Mann and E. G. Straus, Some applications of the Cauchy-Davenport theorem, *Norske Vid. Selsk. Forh. Trondheim* **32** (1959), pp. 74–80.

4. E. Dobrowolski, On a question of Lehmer and the number of irreducible factors of a polynomial, *Acta Arith.* **34** (1979), pp. 391–401.

5. M. M. Dodson, On Waring's problem in $GF[p]$, *Acta Arith.*, **19** (1971), pp.147-173.

6. M. M. Dodson and A. Tietäväinen, A note on Waring's problem in $GF[p]$, *Acta Arith.*, **30** (1976), pp. 159–167.

7. A. Garsia and J. F. Voloch, Fermat curves over finite fields, *J. Number Theory* **30** (1988), pp. 345–356.

8. G. H. Hardy and J. E. Littlewood, Some problems of "Partitio Numerorum". VIII: The number $\Gamma(k)$ in Waring's problem, *Proc. London Math. Soc.* **28**(2) (1927), pp. 518–542.

9. H. Heilbronn, *Lecture notes on additive number theory* mod $p$, Calif. Inst. Technology, Pasadena, CA, 1964.

10. S. V. Konyagin, On estimates of Gaussian sums and Waring's problem for a prime modulus, *Proc. Steklov Inst. of Math. Issue 1,* 1994, pp. 105–117.

11. K. Prachar, *Primzahlverteilung*, Springer–Verlag, Berlin, 1971.

12. A. Tietäväinen, Proof of a conjecture of S. Chowla, *J. Number Theory* **7** (1975), pp. 353–356.

**Apie Varingo problemą pirminiam moduliui**

A. Dubickas

Straipsnyje gautas įvertis iš apačios p-adžioje Varingo problemoje, kai tam tikra sveikųjų skaičių laipsnių suma dalijasi iš pirminio skaičiaus.

Received: September 30, 1999
Accepted: October 27, 1999