Waring’s problem with the Ramanujan $\tau$-function

M. Z. Garaev, V. C. Garcia, and S. V. Konyagin

Abstract. We prove that for every integer $N$ the Diophantine equation $\sum_{i=1}^{74000} \tau(n_i) = N$, where $\tau(n)$ is the Ramanujan $\tau$-function, has a solution in positive integers $n_1, n_2, \ldots, n_{74000}$ satisfying the condition $\max_{1 \leq i \leq 74000} n_i \ll |N|^{2/11} + 1$. We also consider similar questions in residue fields modulo a large prime $p$.

§ 1. Introduction

The Ramanujan function $\tau(n)$ is defined by

$$X \prod_{n=1}^{\infty} (1 - X^n)^{24} = \sum_{n=1}^{\infty} \tau(n)X^n.$$ 

It possesses many remarkable arithmetic properties. It is known that

1) $\tau(n)$ is integer-valued and multiplicative, that is, $\tau(nm) = \tau(n)\tau(m)$ if $\gcd(n,m) = 1$,
2) $\tau(q^{\alpha+2}) = \tau(q^{\alpha+1})\tau(q) - q^{\alpha} \tau(q^\alpha)$ for every integer $\alpha \geq 0$ and every prime $q$ (in particular, $\tau(q^2) = \tau^2(q) - q^{11}$),
3) $\tau(n) \equiv \sum_{d|n} d^{11} \pmod{691}$,
4) $\tau(n) \equiv \sum_{d|n} d^{11} \pmod{2^8}$ for odd $n$,
5) $|\tau(q)| \leq 2q^{11/2}$ for every prime $q$ and $|\tau(n)| \ll n^{11/2+\varepsilon}$ for every positive integer $n$ and any $\varepsilon > 0$ (Deligne [1]).

Here and throughout the paper, the constants in Vinogradov’s symbols $\ll$ and $\gg$ depend only on $\varepsilon$.

Proofs of these and other properties of $\tau(n)$ can be found in [1]–[4]. In particular, one can derive from the results in [4] that any residue class modulo a prime $p$ can be written as $\tau(n) \pmod{p}$ for some positive integer $n$. Using the sum-product estimate of Bourgain, Katz and Tao [5] and Vinogradov’s double exponential sum estimate, Shparlinski [6] established that the values of $\tau(n)$, $n \leq p^4$, form a finite additive basis modulo $p$: there is an integer absolute constant $s \geq 1$ such that every residue class modulo $p$ can be written in the form

$$\tau(n_1) + \cdots + \tau(n_s) \pmod{p},$$

with some positive integers $n_1, \ldots, n_s \leq p^4$. In this paper we use a new approach and reduce the exponent 4 of $p$ to the best possible value of 2/11.

The third author was supported by INTAS (grant no. 03-51-2070), by the Russian Foundation for Basic Research (grant no. 05-01-00066) and by the President’s Programme for the Support of Leading Scientific Schools (grant no. NSh-5813.2006.1).

AMS 2000 Mathematics Subject Classification. 11B83, 11B50, 11P32.
Theorem 1. The set of values of the function $\tau(n)$ forms a finite additive basis for the set of integers. Moreover, for every integer $N$, the Diophantine equation

$$
\sum_{i=1}^{74000} \tau(n_i) = N
$$

has a solution in positive integers $n_1, n_2, \ldots, n_{74000}$ satisfying the condition

$$
\max_{1 \leq i \leq 74000} n_i \ll |N|^{2/11} + 1.
$$

We remark that the number $74000$ arose as $36 \times 2050 + 200$. Here one can reduce the number 2050 (as well as the number 200) using recent developments in the study of the Waring–Goldbach problem \cite{7}, \cite{8}. However, the number of summands remains large. In this direction we prove the following result, where $p$ is assumed to be a large prime.

Theorem 2. For every integer $\lambda$ the congruence

$$
\sum_{i=1}^{16} \tau(n_i) - \sum_{i=1}^{16} \tau(m_i) \equiv \lambda \pmod{p}
$$

holds for some positive integers $n_1, m_1, \ldots, n_{16}, m_{16}$ with

$$
\max_{1 \leq i \leq 16} \{n_i, m_i\} \ll p^2 \log^4 p, \quad \gcd(n_im_i, 23!) = 1.
$$

Using Theorem 2, we can write every residue class modulo $p$ in the form

$$
\sum_{i=1}^{96} \tau(n_i) \pmod{p},
$$

where $\max_{1 \leq i \leq 96} n_i \ll p^2 \log^4 p$. In particular, for some positive constant $C$ the set

$$
\{ \tau(n) \pmod{p} : n \leq Cp^2 \log^4 p \}
$$

forms a finite additive basis for the residue ring $\mathbb{Z}_p$ of order at most 96 (see \cite{9} for a definition).

Theorem 3. For every integer $\lambda$ and every $\varepsilon > 0$, the congruence

$$
\sum_{i=1}^{16} \tau(n_i) \equiv \lambda \pmod{p}
$$

is soluble in positive integers $n_1, \ldots, n_{16}$ satisfying the condition

$$
\max_{1 \leq i \leq 16} n_i \ll p^{3+\varepsilon}.
$$

In particular, the set $\{ \tau(n) \pmod{p} : n \leq p^{3+\varepsilon} \}$ is a basis of $\mathbb{Z}_p$ of order at most 16 for all sufficiently large primes $p$.

In what follows we denote primes by $q, q_1, q_2, \ldots$ and write $|\mathcal{A}|$ for the cardinality of a set $\mathcal{A}$. 
§ 2. Preliminaries

First we recall a corollary of a classical result of Hua Loo-Keng [10].

**Lemma 4.** Let $s_0$ be a fixed integer $\geq 2049$ and let $J$ be the number of solutions of the Waring–Goldbach equation

$$\sum_{i=1}^{s_0} q_i^{11} = N$$

in primes $q_1, \ldots, q_{s_0}$ with $q_i > 23$ for all $i$, $1 \leq i \leq s_0$. Then there are positive constants $c_1 = c_1(s_0)$ and $c_2 = c_2(s_0)$ such that the following estimates hold for all sufficiently large integers $N$ with $N \equiv s_0 \pmod{2}$:

$$c_1 \frac{N^{s_0/11-1}}{(\log N)^{s_0}} \leq J \leq c_2 \frac{N^{s_0/11-1}}{(\log N)^{s_0}}.$$

We shall use the following result of Glibichuk [11].

**Lemma 5.** If $\mathcal{X}, \mathcal{Y} \subset \mathbb{Z}_p$ are subsets with $|\mathcal{X}| |\mathcal{Y}| > 2p$, then

$$\left\{ \sum_{i=1}^{8} x_i y_i : x_i \in \mathcal{X}, y_i \in \mathcal{Y} \right\} = \mathbb{Z}_p.$$

We shall also use some results concerning the values of $\tau(n)$. By Deligne’s result mentioned above we have

$$|\tau(n)| \ll n^{11/2+\varepsilon},$$

and the $N^6$ numbers

$$\sum_{i=1}^{6} \tau(a_i), \quad 1 \leq a_1, \ldots, a_6 \leq N,$

are integers of magnitude $O(N^{11/2+\varepsilon})$. Thus, on average, there are many ways of representing every number as the sum of six values of $\tau(n)$. It is natural to expect that 0 can also be written as the sum of six values of $\tau(n)$. With this observation in mind, we look for six positive integers $a_1, \ldots, a_6$ satisfying

$$\sum_{i=1}^{6} \tau(a_i) = 0.$$

There are many formulae which connect $\tau(n)$ with the function

$$\sigma_s(n) = \sum_{d|n} d^s.$$

For example, it is known that

$$\tau(n) = \frac{65}{756} \sigma_{11}(n) + \frac{691}{756} \sigma_5(n) - \frac{691}{3} \sum_{k=1}^{n-1} \sigma_5(k) \sigma_5(n-k).$$
Another formula states that
\[
\tau(n) = n^4\sigma_0(n) - 24 \sum_{k=1}^{n-1} (35k^4 - 52k^3n + 18k^2n^2)\sigma_0(k)\sigma_0(n-k)
\]
(see [12]). Formulae of this type are useful in the numerical calculation of \(\tau(n)\). In particular, one can deduce that
\[
\tau(12) = -370944, \quad \tau(27) = -73279080, \quad \tau(55) = 2582175960,
\]
\[
\tau(69) = 4698104544, \quad \tau(90) = 13173496560, \quad \tau(105) = -20380127040.
\]
Thus we have
\[
\tau(12) + \tau(27) + \tau(55) + \tau(69) + \tau(90) + \tau(105) = 0. \quad (1)
\]
Now, assuming that Theorem 2 is true, we multiply the equation of sets
\[
\left\{ \sum_{i=1}^{16} \tau(n_i) - \sum_{i=1}^{16} \tau(m_i) \pmod{p} : m_i, n_i \leq Cp^2\log^4 p, \gcd(m_i n_i, 23!) = 1 \right\} = \mathbb{Z}_p
\]
by \(\tau(12)\). Since
\[
\tau(12) \left( \sum_{i=1}^{16} \tau(n_i) - \sum_{i=1}^{16} \tau(m_i) \right) = \sum_{i=1}^{16} \tau(12)\tau(n_i)
\]
\[
+ (\tau(27) + \tau(55) + \tau(69) + \tau(90) + \tau(105)) \sum_{i=1}^{16} \tau(m_i),
\]
we see from the multiplicative property of \(\tau(n)\) that the set
\[
\left\{ \tau(n) \pmod{p} : n \leq Cp^2\log^4 p \right\}
\]
is an additive basis in \(\mathbb{Z}_p\) of order at most 96.

It is also useful to note that
\[
\tau(6) = -6048, \quad \tau(14) = 401856, \quad \tau(29) = 128406630, \quad \tau(41) = 308120442,
\]
\[
\tau(42) = 101267712, \quad \tau(44) = -786948864, \quad \tau(48) = 248758272.
\]
Thus we can write 0 as the sum of seven values of \(\tau(n)\):
\[
\tau(6) + \tau(14) + \tau(29) + \tau(41) + \tau(42) + \tau(44) + \tau(48) = 0. \quad (2)
\]

§ 3. Proof of Theorem 1

Let \(M\) be a large even parameter and write
\[
\mathcal{Q} = \{q : 23 < q \leq M^{1/11}\}.
\]
A subset $\mathcal{Q}' \subset \mathcal{Q}$ is said to be \textit{admissible} if the equation
\[
\sum_{i=1}^{6} \tau(q'_i) = \sum_{i=7}^{12} \tau(q'_i)
\]
has no solutions $q'_1, \ldots, q'_{12} \in \mathcal{Q}'$ satisfying the conditions
\[
q'_1 < \cdots < q'_6, \quad q'_7 < \cdots < q'_{12}, \quad (q'_1, \ldots, q'_6) \neq (q'_7, \ldots, q'_{12}).
\]
Using various properties of the function $\tau(n)$, one can easily verify that there are admissible subsets of 12 elements. To do this, combine the above congruences
\[
\tau(q) \equiv 1 + q^{11} \pmod{691}, \quad \tau(q) \equiv 1 + q^{11} \pmod{2^8},
\]
where $q$ is an odd prime, with the Chinese remainder theorem and Dirichlet’s theorem for primes in arithmetic progressions. It follows that for every $j$ with $1 \leq j \leq 12$ one can find a sufficiently large prime $\ell_j$ satisfying
\[
\tau(\ell_j) \equiv 2^j \pmod{8 \times 691}.
\]
We now consider an admissible subset $\mathcal{Q}'$ of the largest possible cardinality. If there are several such subsets, we take any one of them. In particular, $|\mathcal{Q}'| \geq 12$ and all the sums
\[
\sum_{i=1}^{6} \tau(q'_i), \quad q'_1 < \cdots < q'_6, \quad q'_1, \ldots, q'_6 \in \mathcal{Q}',
\]
are distinct. Using Deligne’s estimate for $\tau(q)$ and the pigeonhole principle, we have
\[
|\mathcal{Q}'|^6 \ll (M^{1/11})^{11/2},
\]
whence
\[
|\mathcal{Q}'| \ll M^{1/11 - 1/132}.
\]
Given $q \in \mathcal{Q} \setminus \mathcal{Q}'$, consider the set $\mathcal{Q}' \cup \{q\}$. Since $|\mathcal{Q}'|$ is maximal, there are $q'_1, \ldots, q'_{12} \in \mathcal{Q}' \cup \{q\}$ such that
\[
\sum_{i=1}^{6} \tau(q'_i) = \sum_{i=7}^{12} \tau(q'_i),
\]
\[
q'_1 < \cdots < q'_6, \quad q'_7 < \cdots < q'_{12}, \quad (q'_1, \ldots, q'_6) \neq (q'_7, \ldots, q'_{12}).
\]
The definition of $\mathcal{Q}'$ implies that
\[
q \in \{q'_1, \ldots, q'_{12}\}.
\]
Moreover, (6) shows that the number $q$ occurs at most twice in the sequence $q'_1, \ldots, q'_{12}$. If it does occur twice, then it occurs once in the sequence $q'_1, \ldots, q'_6$ and once in the sequence $q'_7, \ldots, q'_{12}$. Therefore we can subtract $\tau(q)$ from both sides of (5) and renumber the remaining $q'_i$. It follows that there are elements
\[
q'_1, \ldots, q'_5 \in \mathcal{Q}', \quad q'_7, \ldots, q'_{11} \in \mathcal{Q}'
\]
such that
\[ \sum_{i=1}^{5} \tau(q'_i) = \sum_{i=7}^{11} \tau(q'_i), \]
\[ q'_1 < \cdots < q'_5, \quad q'_7 < \cdots < q'_{11}, \quad (q'_1, \ldots, q'_5) \neq (q'_7, \ldots, q'_{11}). \] (8)

Since \(|Q'| > 10\), there is a number \(q' \in Q' \setminus \{q'_1, \ldots, q'_5, q'_7, \ldots, q'_{11}\}\). (9)

Then
\[ \sum_{i=1}^{5} \tau(q'_i) + \tau(q') = \sum_{i=7}^{11} \tau(q'_i) + \tau(q'). \]

This contradicts the definition of \(Q'\) because of (7)–(9).

Therefore the only possible case is when \(q\) occurs exactly once in the sequence \(q'_1, \ldots, q'_{12}\). Thus, in view of (5), there are \(\tilde{q}_1, \ldots, \tilde{q}_{11} \in Q'\) such that
\[ \sum_{i=1}^{6} \tau(\tilde{q}_i) = \sum_{i=7}^{11} \tau(\tilde{q}_i) + \tau(q). \]

Hence the following equations hold for all \(q \in Q \setminus Q'\):
\[ \sum_{i=1}^{6} \tau(\tilde{q}_i) - \sum_{i=7}^{11} \tau(\tilde{q}_i) - \tau(q^2) = \tau(q) \sum_{i=1}^{6} \tau(\tilde{q}_i) - \tau(q) \sum_{i=7}^{11} \tau(\tilde{q}_i) - \tau(q^2) \]
\[ = \tau^2(q) - \tau(q^2) = q^{11}. \] (10)

Thus we have proved that for every element \(q \in Q \setminus Q'\) there are elements \(\tilde{q}_1, \ldots, \tilde{q}_{11} \in Q'\) such that
\[ q^{11} = \sum_{i=1}^{6} \tau(\tilde{q}_i) - \sum_{i=7}^{11} \tau(\tilde{q}_i) - \tau(q^2). \] (10)

Our next aim is to prove that the Waring–Goldbach equation
\[ \sum_{j=1}^{2050} q_j^{11} = M \] (11)
is soluble in primes \(q_1, \ldots, q_{2050} \in Q \setminus Q'\). First, we have \(q_j \leq M^{1/11}\) by (11). Lemma 4 with \(s_0 = 2050\) yields the following lower bound for the number \(I\) of solutions of (11) satisfying \(q_j \in Q\):
\[ I \geq c_1 \frac{M^{2050/11-1}}{(\log M)^{2050}}. \] (12)

Lemma 4 with \(s_0 = 2049\) and (4) yield the following upper bound for the number \(J\) of solutions of (11) with at least one \(q_{j_0} \in Q'\):
\[ J \leq 2050 c_2 |Q'| M^{2049/11-1} (\log M)^{2049} \leq M^{2050/11-1/132} (\log M)^{2049}. \] (13)
Thus $I > J$. It follows that equation (11) has a solution with all $q_j \in \mathcal{O} \setminus \mathcal{O}'$. We fix such a solution $q_1, \ldots, q_{2050}$. Apply (10) with $q = q_j$ to each $q_j$ with $1 \leq j \leq 2050$ and sum the results. Since $\tilde{q}_i q \leq M^{2/11}$, we get

$$M = \sum_{i=1}^{6 \times 2050} \tau(n_i) - \sum_{i=1}^{6 \times 2050} \tau(m_i),$$

where

$$\max_{1 \leq i \leq 6 \times 2050} \{n_i, m_i\} \leq M^{2/11}, \quad \gcd(n_i m_i, 23!) = 1.$$

We assumed $M$ to be large and even. Multiplying both sides of (14) by $-1$, we get a similar representation for $-M$. Moreover, we can admit $M$ of either parity by replacing $M$ by $M - \tau(1)$ or $M - \tau(29)$. Thus every integer $M$ with $|M|$ sufficiently large can be written in the form

$$M = \sum_{i=1}^{6 \times 2050} \tau(n_i) - \sum_{i=1}^{6 \times 2050+1} \tau(m_i),$$

where

$$\max_{1 \leq i \leq 6 \times 2050+1} \{n_i, m_i\} \leq |M|^{2/11} + 1, \quad \gcd(n_i m_i, 23!) = 1.$$

We recall (see (1)) that

$$-\tau(12) = 370944 = \tau(27) + \tau(55) + \tau(69) + \tau(90) + \tau(105).$$

Therefore, multiplying (15) by $-\tau(12)$ and using the multiplicative property of the function $\tau(n)$, we obtain

$$370944M = \sum_{i=1}^{6 \times 6 \times 2050+1} \tau(n_i)$$

with $\max_{1 \leq i \leq 6 \times 6 \times 2050+1} n_i \leq 106|M|^{2/11}$.

We claim that every integer $r$ with $0 \leq r < 370944$ can be written as the sum of, say, exactly 198 numbers $\tau(n)$, $n \leq 105$ (extra effort could reduce 198 to a much smaller constant, but this does not essentially influence our result). Indeed, we recall that

$$\tau(1) = 1, \quad \tau(2) = -24, \quad \tau(3) = 252, \quad \tau(5) = 4830, \quad \tau(8) = 84480.$$

If $0 \leq r < 370944$, then

$$r = 84480r_5 + r'_4 = \tau(8)r_5 + r'_4$$

for some integers $r_5$ and $r'_4$ with $0 \leq r_5 \leq 4$ and $0 \leq r'_4 < 84480$. Every such number $r'_4$ may be written in the form

$$r'_4 = 4830r_4 + r'_3 = \tau(5)r_4 + r'_3,$$
where $0 \leq r_4 \leq 17$ and $0 \leq r'_3 < 4830$. Every such number $r'_3$ may be written in the form

$$r'_3 = 252r_3 - r'_2 = \tau(3)r_3 - r'_2,$$

where $0 \leq r_3 \leq 20$ and $0 \leq r'_2 < 252$. Every such number $r'_2$ may be written in the form

$$r'_2 = 24r_2 - r_1 = -\tau(2)r_2 - r_1,$$

where $0 \leq r_2 \leq 11$ and $0 \leq r_1 < 24$. Thus we get

$$r = \tau(8)r_5 + \tau(5)r_4 + \tau(3)r_3 + \tau(2)r_2 + r_1.$$

Hence we have the desired representation of $r$ with at most

$$r_5 + \cdots + r_1 \leq 75$$

summands $\tau(n)$, $n \leq 10$. On the other hand, every integer greater than 29 can be written in the form $6x + 7y$ for some non-negative integers $x, y$. Thus we can use the constructions (1) and (2) to get a fixed number of summands for all $r$. In particular, every integer $r$ with $0 \leq r < 370944$ can be represented in the form

$$\sum_{i=1}^{198} \tau(a_i)$$

for some positive integers $a_1, \ldots, a_{198} \leq 105$.

Now let $N$ be an arbitrary integer with $|N|$ sufficiently large. By the argument above, there are positive integers $a_1, \ldots, a_{199} \leq 105$ such that

$$N \equiv \sum_{i=1}^{198} \tau(a_i) \pmod{370944}.$$

Using (16), we deduce that

$$N = \sum_{i=1}^{198} \tau(a_i) + 370944M = \sum_{i=1}^{6 \times 6 \times 2050 + 199} \tau(n_i) = \sum_{i=1}^{73999} \tau(n_i),$$

where

$$\max_{1 \leq i \leq 73999} n_i \leq 106|M|^{2/11} \leq 15N^{2/11}.$$

Thus we have proved the existence of an absolute positive integer constant $N_0$ such that the equation

$$\sum_{i=1}^{73999} \tau(n_i) = N$$

has a solution in positive integers $n_1, \ldots, n_{73999} \ll |N|^{2/11}$ for every integer $N$ with $|N| \geq N_0$.

Now let $N$ be an arbitrary integer. If $|N| > N_0$, then $|N - \tau(1)| \geq N_0$ and, therefore, we can express the number $N - \tau(1)$ as the sum of 73999 values of $\tau(n)$ with $n \ll |N|^{2/11}$. Theorem 1 is proved in this case.
If \( |N| \leq N_0 \), then we take an integer constant \( n_0 \) such that \( |\tau(n_0)| > 2N_0 \). Then
\[
|N - \tau(n_0)| > N_0.
\]
Thus \( N - \tau(n_0) \) can be expressed as the sum of 73999 values of \( \tau(n) \), \( n \ll 1 \). Theorem 1 is proved.

**Remark 1.** The numbers \( n_i \) constructed in the proof of Theorem 1 are easily seen to satisfy the condition
\[
\tau(n_i) \ll |N|.
\]

**Remark 2.** We shall prove in a forthcoming paper that, for every integer \( N \) with \( |N| \geq 2 \), the Diophantine equation
\[
\sum_{i=1}^{148000} \tau(n_i) = N
\]
has a solution in positive integers \( n_1, n_2, \ldots, n_{148000} \) satisfying the condition
\[
\max_{1 \leq i \leq 148000} n_i \ll |N|^{2/11} e^{-c \log |N|/\log \log |N|}
\]
for some absolute constant \( c > 0 \). By Deligne’s estimate we have \( \tau(n) \ll n^{11/2}d(n) \), where \( d(n) \) is the number of divisors of \( n \). This condition corresponds to the best possible bound for the size of the variables \( n_i \), apart from the value of the constant \( c \).

### § 4. Proof of Theorem 2

Let \( C \) be a large positive constant. We define the sets
\[
\mathcal{D} = \{ q : 23 < q \leq Cp^{1/2} \log p \},
\]
\[
\mathcal{I} = \{ \tau(q) \pmod{p} : q \in \mathcal{D} \}.
\]
If \( |\mathcal{I}| > 3\sqrt{p} \), then \( \mathcal{I} \) can be divided into subsets \( \mathcal{X}, \mathcal{Y} \) such that \( |\mathcal{X}| |\mathcal{Y}| > 2p \). Then the desired result follows from Lemma 5.

We now consider the case when \( |\mathcal{I}| < 3\sqrt{p} \). Then
\[
\mathcal{D} = \bigcup_{i=1}^{|\mathcal{I}|} \mathcal{A}_i,
\]
where the sets \( \mathcal{A}_i \) are defined in such a way that \( \tau(q') \equiv \tau(q'') \pmod{p} \) whenever \( q', q'' \in \mathcal{A}_i \).

Clearly, there is a subset \( \mathcal{A}_i' \subset \mathcal{A}_i \) such that
\[
0 \leq |\mathcal{A}_i| - |\mathcal{A}_i'| \leq 3, \quad |\mathcal{A}_i'| \equiv 0 \pmod{4}.
\]

Put
\[
\mathcal{D}' = \bigcup_{i=1}^{\frac{|\mathcal{I}|}{3}} \mathcal{A}_i'.
\]
By the prime number theorem, we have \(|\mathcal{D}| \geq Cp^{1/2}\) if \(p\) is sufficiently large. Then
\[
|\mathcal{D}'| \geq |\mathcal{D} - 3| |\mathcal{I}| \geq |\mathcal{D} - 9p^{1/2} \geq (C - 9)p^{1/2}.
\] (17)

Since the cardinality of each of the \(\mathcal{A}_i'\) is even, we can find \(|\mathcal{A}_i'|/2\) pairs of distinct primes belonging to \(\mathcal{A}_i'\). In total we have
\[
\sum_{i=1}^{\mathcal{I}} |\mathcal{A}_i'|/2 = |\mathcal{I}|/2
\]
pairs \((q, q')\). We divide this set of pairs into disjoint subsets \(J_1\) and \(J_2\) with \(|J_1| = |J_2| = |\mathcal{I}|/4\). Consider the sets
\[
\mathcal{X} = \{\tau(qq') - \tau(q^2) \pmod{p} : (q, q') \in J_1\},
\]
\[
\mathcal{Y} = \{\tau(qq') - \tau(q^2) \pmod{p} : (q, q') \in J_2\}.
\]

Since
\[
\tau(qq') - \tau(q^2) = \tau(q)\tau(q') - \tau(q^2) \equiv \tau^2(q) - \tau(q^2) \equiv q^{11} \pmod{p}
\]
and \(q^{11} \pmod{p}\) takes each of its values at most 11 times, we get
\[
|\mathcal{X}| \geq |J_1|/11 = |\mathcal{I}|/44, \quad |\mathcal{Y}| \geq |J_2|/11 \geq |\mathcal{I}|/44.
\]

Therefore, choosing \(C = 100\) (for example), we see from (17) that \(|\mathcal{X}| \cdot |\mathcal{Y}| > 2p\).

Applying Lemma 5, we complete the proof of Theorem 2.

\[\text{§ 5. Proof of Theorem 3}\]

Consider the set of residue classes
\[
\mathcal{A}' = \{\tau(q) \pmod{p} : p/2 < q \leq p\}.
\]

Given \(a' \in \mathcal{A}'\), we write \(I(a')\) for the number of solutions of the congruence
\[
\tau(q) \equiv a' \pmod{p}, \quad p/2 < q \leq p.
\]

By the prime number theorem we have
\[
\sum_{a' \in \mathcal{A}'} I(a') = \sum_{p/2 < q \leq p} 1 \gg p \log^{-1} p.
\]

Hence there is an \(a_0' \in \mathcal{A}'\) such that
\[
I(a_0') \gg p|\mathcal{A}'|^{-1} \log^{-1} p.
\] (18)

We put \(\mathcal{A} = \mathcal{A}' \setminus \{a_0'\}\) if \(|\mathcal{A}'| \geq 2\) and \(\mathcal{A} = \{\tau(1)\} = \{1\}\) if \(|\mathcal{A}'| = 1\). Then
\[
|\mathcal{A}'|/2 \leq |\mathcal{A}| \leq |\mathcal{A}'|.
\] (19)
We define the set
\[ \mathcal{B} = \{ \tau(q^2) \pmod{p} : p/2 < q \leq p, \tau(q) \equiv a_0' \pmod{p} \}. \]

The elements of \( \mathcal{B} \) are given by
\[ \tau(q^2) = \tau^2(q) - q^{11} \equiv (a_0')^2 - q^{11} \pmod{p}, \]
where \( p/2 < q \leq p \) and \( \tau(q) \equiv a_0' \pmod{p} \). Thus, according to (18) and (19), the number \( q \) can take any value in a set containing
\[ \gg p|\mathcal{A}'|^{-1} \log^{-1} p \gg p|\mathcal{A}|^{-1} \log^{-1} p \]
distinct residue classes modulo \( p \). Since \( q^{11} \pmod{p} \) takes each of its values at most 11 times, we have
\[ |\mathcal{B}| \gg p|\mathcal{A}'|^{-1} \log^{-1} p. \]  

Choose an arbitrary \( \varepsilon \) with \( 0 < \varepsilon < 0.1 \). Let \( \mathcal{C} \) be the set of distinct elements of the sequence
\[ \tau(q) \pmod{p}, \ \tau(q^2) \pmod{p}, \]
where \( q \leq p^{0.5\varepsilon} \). Applying the above argument to the sets
\[ \{ \tau(q) \pmod{p} : q \leq p^{0.5\varepsilon} \}, \]
\[ \{ \tau(q^2) \pmod{p} : q \leq p^{0.5\varepsilon} \}, \]
we see that \( |\mathcal{C}| \gg p^{\varepsilon/6} \). Note that the sets \( \mathcal{A}, \mathcal{B}, \mathcal{C} \) are made up of elements of the form \( \tau(n_1), \tau(n_2), \tau(n_3) \) respectively in such a way that \( n_1, n_2, n_3 \) are pairwise coprime and \( n_1 \leq p, n_2 \leq p^2, n_3 \leq p^\varepsilon \).

If \( |\mathcal{A}| < p^{0.1\varepsilon} \), then \( |\mathcal{B}| \gg p^{1-\varepsilon/9} \) by (20) and, therefore, \( |\mathcal{B}|/|\mathcal{C}| \gg p^{1+0.01\varepsilon} \). Hence we can apply Lemma 5 with \( \mathcal{X} = \mathcal{B} \) and \( \mathcal{Y} = \mathcal{C} \) and use the multiplicative property of \( \tau(n) \). The elements of the set
\[ \mathcal{X} \mathcal{Y} = \{ xy : x \in \mathcal{X}, y \in \mathcal{Y} \} \]
in this case will be of the form \( \tau(n) \pmod{p} \), where \( n \leq p^{2+\varepsilon} \).

If \( |\mathcal{A}| > p^{2/3} \), then we divide \( \mathcal{A} \) into disjoint subsets \( \mathcal{A}_1 \) and \( \mathcal{A}_2 \) with \( \gg p^{2/3}/3 \) elements in each. Apply Lemma 5 with \( \mathcal{X} = \mathcal{A}_1 \) and \( \mathcal{Y} = \mathcal{A}_2 \). In this case, the elements of the set \( \mathcal{X} \mathcal{Y} \) are of the form \( \tau(n) \pmod{p} \), where \( n \leq p^2 \).

If \( p^{\varepsilon/10} \ll |\mathcal{A}| \ll p^{2/3} \), then we write \( \mathcal{T} \) for whichever of \( \mathcal{A} + \mathcal{C} \) and \( \mathcal{A} \mathcal{C} \) has the larger cardinality. Since \( |\mathcal{C}| \gg p^\varepsilon/6 \), Bourgain’s estimate ([13], Theorem 1.1) implies that there is a positive constant \( \gamma = \gamma(\varepsilon) > 0 \) such that
\[ |\mathcal{T}| \gg p^\gamma |\mathcal{A}|. \]

Then \( |\mathcal{B}|/|\mathcal{T}| \gg p^{1+\gamma/2} \). Hence we can apply Lemma 5 with \( \mathcal{X} = \mathcal{B} \) and \( \mathcal{Y} = \mathcal{T} \). In this case, the elements of the set \( \mathcal{X} \mathcal{Y} \) are either of the form \( \tau(n_1) + \tau(n_2) \pmod{p} \) with \( n \leq p^3 \) or of the form \( \tau(n) \pmod{p} \) with \( n \leq p^{3+\varepsilon} \). This proves Theorem 3.
Bibliography

[1] P. Deligne, “La conjecture de Weil. I”, Inst. Hautes Études Sci. Publ. Math., 1974, no. 43, 273–307; Russian transl., Uspekhi Mat. Nauk 30:5 (1975), 159–190.

[2] H. Iwaniec, Topics in classical automorphic forms, Grad. Stud. Math., Amer. Math. Soc., Providence, RI 1997.

[3] N. Koblitz, Introduction to elliptic curves and modular forms, Grad. Texts in Math., vol. 97, Springer-Verlag, New York 1984; Russian transl., Mir, Moscow 1988.

[4] J.-P. Serre, “Congruences et formes modulaires [d’après H. P. F. Swinnerton-Dyer]”, Séminaire Bourbaki, 24e année (1971/1972), exp. no. 416, Lecture Notes in Math., vol. 317, Springer, Berlin 1973, pp. 319–338; Russian transl., Uspekhi Mat. Nauk 28:2 (1973), 183–196.

[5] J. Bourgain, N. Katz, and T. Tao, “A sum-product estimate in finite fields and applications”, Geom. Funct. Anal. 14:1 (2004), 27–57.

[6] I. E. Shparlinski, “On the value set of the Ramanujan function”, Arch. Math. 85:6 (2005), 508–513.

[7] G. I. Arkhipov and V. N. Chubarikov, “On the number of summands in Vinogradov’s additive problem and its generalizations”, Proc. IV Internat. Conf. “Modern problems of number theory and its applications”: Current problems, part I (Tula, Russia, 10–15 September 2001) (V. N. Chubarikov et al., eds.), Moscow State Univ., Dept. Math. and Mech., Moscow 2002, pp. 5–38. (Russian)

[8] A. V. Kumchev and D. I. Tolev, “An invitation to additive prime number theory”, Serdica Math. J. 31:1–2 (2005), 1–74.

[9] A. A. Karatsuba, “Additive congruences”, Izv. Ross. Akad. Nauk Ser. Mat. 61:2 (1997), 81–94; English transl., Izv. Math. 61:2 (1997), 317–329.

[10] Hua Loo-Keng, Additive prime number theory, Trudy Mat. Inst. Steklova, vol. 22, 1947. (Russian)

[11] A. A. Glibichuk, “Combinational properties of sets of residues modulo a prime and the Erdős–Graham problem”, Mat. Zametki 79:3 (2006), 384–395; English transl., Math. Notes 79:3–4 (2006), 356–365.

[12] D. Niebur, “A formula for Ramanujan’s $\tau$-function”, Illinois J. Math. 19 (1975), 448–449.

[13] J. Bourgain, “More on the sum-product phenomenon in prime fields and its applications”, Int. J. Number Theory 1:1 (2005), 1–32.

M. Z. Garaev
Instituto de Matemáticas UNAM,
C. P. 58089, Morelia, Michoacán, México
E-mail: garaev@matmor.unam.mx

V. C. García
Instituto de Matemáticas UNAM,
C. P. 58089, Morelia, Michoacán, México
E-mail: garci@matmor.unam.mx

S. V. Konyagin
Department of Mechanics and Mathematics,
Moscow State University
E-mail: konyagin@ok.ru