On the Parity of Additive Representation Functions

J.-L. Nicolas*

Institut Girard Desargues, UPRES-A 5028, Bât. 101, Université Claude Bernard (Lyon I),
F-69622 Villeurbanne Cedex, France
E-mail: jlnicola@in2p3.fr

I. Z. Ruzsa*

Mathematical Institute of the Hungarian Academy of Sciences,
Pf. 127, H-1364 Budapest, Hungary
E-mail: rusza@math-inst.hu

and

A. Sárközy*

Department of Algebra and Number Theory, Eötvös Loránd University,
Museum krt. 6-8, H-1088 Budapest, Hungary
E-mail: sarkozy@cs.elte.hu

Communicated by A. Hildebrand

Received November 10, 1997; revised March 20, 1998

Let $A$ be a set of positive integers, $p(A, n)$ be the number of partitions of $n$ with
parts in $A$, and $p(n) = p(N, n)$. It is proved that the number of $n \leq N$ for which $p(n)$
is even is $\gg \sqrt{N}$, while the number of $n \leq N$ for which $p(n)$ is odd is $\gg N^{1/2 + \epsilon(1)}$.
Moreover, by using the theory of modular forms, it is proved (by J.-P. Serre) that,
for all $a$ and $m$ the number of $n$, such that $n = a \pmod{m}$, and $n \leq N$ for which
$p(n)$ is even is $\gg c \sqrt{N}$ for any constant $c$, and $N$ large enough. Further a set $A$
is constructed with the properties that $p(A, n)$ is even for all $n \geq 4$ and its counting
function $A(x)$ (the number of elements of $A$ not exceeding $x$) satisfies $A(x) \gg x \log x$. Finally, we study the counting function of sets $A$ such that the number of
solutions of $a + a' = n, a, a' \in A, a < a'$ is never 1 for large $n$. © 1998 Academic Press
Z and N denote the set of the integers, resp. positive integers. \( \mathcal{A}, \mathcal{B}, ... \)
will denote sets of positive integers, and their counting functions will be
denoted by \( A(x), B(x), ... \) so that, e.g.,
\[
A(x) = |\{ a: a \leq x, a \in \mathcal{A}\}|
\]
If \( a, b \in \mathbb{N} \), \([a, b)\) will denote the set of the integers \( n \) such that \( a \leq n < b \).
If \( \mathcal{A} = \{a_1, a_2, ...\} \subset \mathbb{N} \) (where \( a_1 < a_2 < \ldots \) ), then \( p(\mathcal{A}, n) \) denotes the
number of solutions of the equation
\[
a_1x_1 + a_2x_2 + \cdots = n
\]
in non-negative integers \( x_1, x_2, ... \) and, in particular, \( p(n) \) (= \( p(\mathbb{N}, n) \))
denotes the number of unrestricted partitions of \( n \). Moreover, the number of solutions of
\[
a_i + a_j = n, \quad i \leq j
\]
will be denoted by \( r(\mathcal{A}, n) \). Ramanujan initiated the study of the parity of
the numbers \( p(n) \). Kolberg \([2]\) proved that \( p(n) \) assumes both even and odd
values infinitely often. Improving on an estimate of Mirsky \([4]\), Nicolas
and Sárközy \([5]\) proved that there are at least \( (\log N)^c \) \((c > 0)\) numbers \( n \)
such that \( n \in \mathbb{N} \) and \( p(n) \) is even, and there are at least \( (\log N)^c \) numbers
\( m \in \mathbb{N} \) such that \( p(m) \) is odd. Moreover, they extended the problems by
proposing the study of the parity of the functions \( p(\mathcal{A}, n) \) and \( r(\mathcal{A}, n) \) for
\( \mathcal{A} \subset \mathbb{N} \). (See \([5]\) and \([6]\) for further references.)

In this paper first we will improve on the result of Nicolas and Sárközy
mentioned above:

**Theorem 1.** There are absolute constants \( c_1 > 0 \), \( N_0 \), such that if \( N > N_0 \),
then there are at least \( c_1N^{1/2} \) integers \( n \) for which \( n \in \mathbb{N} \) and \( p(n) \) is even.

**Theorem 2.** For all \( \varepsilon > 0 \) there is a number \( N_1 = N_1(\varepsilon) \) such that if \( N > N_1 \),
then there are at least \( N^{1/2} \exp(-\log 2 + \varepsilon) \log N/\log \log N \) integers \( n \) for
which \( n \in \mathbb{N} \) and
\[
p(n) \not\equiv p(n - 1) \pmod{2}
\]
(and consequently the same lower bound holds for the number of integers \( n \)
for which \( n \in \mathbb{N} \) and \( p(n) \) is odd).

Subbarao \([11]\) conjectured that every infinite arithmetic progression
\( r, r + q, r + 2q, ... \) of positive integers contains infinitely many integers \( m \) for
which \( p(m) \) is odd, and it contains infinitely many integers \( n \) for which \( p(n) \) is even. For special values of \( r \) and \( q \), this conjecture has been proved by Garvan, Kolberg, Hirschhorn, Stanton, and Subbarao. Ono [6] has proved that for all \( r, q \) there are infinitely many integers \( n \equiv r \pmod{q} \) for which \( p(n) \) is even, moreover, in any arithmetic progression \( r, r+q, r+2q, \ldots \) there are infinitely many integers \( m \equiv r \pmod{q} \) for which \( p(m) \) is odd, provided there is one such \( m \). As pointed out by J.-P. Serre, it is possible to prove the following quantitative version of the first half of Ono’s theorem:

**Theorem 3.** If \( r \) is an integer and \( q \in \mathbb{N}, q \geq 1 \) then, for any positive real number \( c_2 \), there is a constant \( N_2 = N_2(c_2, q) > 0 \) such that for \( N > N_2 \) there are at least \( c_2 N^{1/2} \) integers \( n \) for which \( n \not\equiv r \pmod{q} \) and \( p(n) \) is even.

Note that Theorem 1 is weaker than Theorem 3, however, it can be handled elementarily, while in order to prove Theorem 3 one needs a result of Serre on modular forms ([8, 9]). Recently, Ahlgren ([1]) has given a proof of a Theorem slightly weaker than Theorem 3, and has also proved a quantitative version of Ono’s Theorem about the odd values of the partition function. More precisely, Ahlgren has proved that, for all \( r \) and \( q \), if there exists an \( m \not\equiv r \pmod{q} \) for which \( p(m) \) is odd, then

\[
\# \{n \leq X, n \equiv r \pmod{q}, p(n) \text{ is odd} \} \gg \sqrt{X}/\log X.
\]

In the Appendix, J.-P. Serre will give a proof of Theorem 3 in a larger frame dealing with the parity of the coefficients of any modular form.

In the second half of this paper we will study the following problem:

As we pointed out in [5], there are infinitely many infinite sets \( \mathcal{A}, \mathcal{B}, \mathcal{C} \) and \( \mathcal{D} \) such that \( p(\mathcal{A}, n) \), resp. \( r(\mathcal{B}, n) \) is even, while \( p(\mathcal{C}, n) \), resp. \( r(\mathcal{D}, n) \) is odd from a certain point on; indeed, as the proof of Theorem 4 will show, any finite set \( \mathcal{E} = \{e_1, \ldots, e_k\} \subset \mathbb{N} \) (where \( e_1 < \cdots < e_k \)) can be extended to an infinite set \( \mathcal{A}, \mathcal{B}, \mathcal{C} \) or \( \mathcal{D} \) of the type described above so that \( \mathcal{A} \cap [1, e_2] = \mathcal{E}, \mathcal{B} \cap [1, e_2] = \mathcal{E}, \mathcal{C} \cap [1, e_2] = \mathcal{E}, \) resp. \( \mathcal{D} \cap [1, e_2] = \mathcal{E} \).

But what can one say on such a set \( \mathcal{A}, \mathcal{B}, \mathcal{C} \) or \( \mathcal{D} \)? In particular, how thin, or how dense can be a set of this type?

In case of the function \( p(\mathcal{A}, n) \), all we can show is that there is a set of \( \mathcal{A} \) for which \( A(x) \gg x/\log x \) and \( p(\mathcal{A}, n) \) is even from a certain point on:

**Theorem 4.** There is an infinite set \( \mathcal{A} \subset \mathbb{N} \) such that

\[
p(\mathcal{A}, n) \text{ is even for } n \geq 4
\]

and

\[
\liminf_{x \to +\infty} \frac{A(x) \log x}{x} \geq \frac{1}{2}.
\]
Studying the parity of the function \( r(\mathcal{A}, n) \), one may start out from the following observation: if \( r(\mathcal{A}, n) \) is odd for \( n \geq n_0 \), then certainly

\[
    r(\mathcal{A}, n) \neq 0 \quad \text{for} \quad n \geq n_0. \tag{1.3}
\]

This implies that \( \mathcal{A} \) cannot be very thin. Indeed, a trivial counting argument gives that if

\[
    \liminf_{x \to +\infty} \frac{A(x)}{x^{1/2}} < \sqrt{2}
\]

then

\[
    r(\mathcal{A}, n) = 0
\]

infinitely often. On the other hand, it is known that there is an asymptotic basis \( \mathcal{A} \) of order 2 such that

\[
    \limsup_{x \to +\infty} \frac{A(x)}{x^{1/2}} < +\infty
\]

(see Stöhr [10]). Thus we may conclude relatively easily that if \( \mathcal{A} \) is a set of property (1.3) then \( A(x) \) must grow as fast as \( cx^{1/2} \), and this is the best possible apart from the value of \( c \).

We obtain a much more interesting question making the “even analog” of this observation. Indeed, if \( r(\mathcal{A}, n) \) is even for \( n \geq n_0 \), then certainly

\[
    r(\mathcal{A}, n) \neq 1 \quad \text{for} \quad n \geq n_0.
\]

This implies that

\[
    \liminf_{x \to +\infty} \frac{A(x) \log 2}{\log x} \geq 1 \tag{1.4}
\]

since otherwise, writing \( \mathcal{A} = \{a_1, a_2, \ldots \} \) (where \( a_1 < a_2 < \cdots \)) we had

\[
    2a_k < a_{k+1}
\]

infinitely often, and for such a \( k \) we have

\[
    r(\mathcal{A}, 2a_k) = 1.
\]

So the question is whether (1.4) can be improved; how far is it from the best possible? We shall be able to improve it to \( A(x) \gg (\log x)^{3/2-\varepsilon} \) and, on the other hand, we will show that \( A(x) \ll (\log x)^2 \) is possible.
Theorem 5. If \( \mathcal{A} \) is an infinite set of positive integers such that there is a number \( n_0 \) with

\[
r(\mathcal{A}, n) \neq 1 \quad \text{for} \quad n \geq n_0 \quad (1.5)
\]
then we have

\[
\limsup_{x \to +\infty} \frac{A(x)(\log \log x)^{3/2}}{(\log x)^{1/4}} \geq \frac{1}{20}. \quad (1.6)
\]

Theorem 6. There is an infinite set \( \mathcal{A} \subset \mathbb{N} \) such that

\[
\limsup_{x \to +\infty} \frac{A(x)}{(\log x)^2} < +\infty \quad (1.7)
\]
and there is a number \( n_0 \) with

\[
r(\mathcal{A}, n) \neq 1 \quad \text{for} \quad n \geq n_0. \quad (1.8)
\]

2

Proof of Theorem 1. Set \( p(0) = 1 \) and \( p(-1) = p(-2) = \cdots = 0 \). As in [5], we start out from Euler’s identity

\[
\sum_{j=0}^{+\infty} \varepsilon_j p(n-u_j) = 0 \quad \text{(for all} \ n \in \mathbb{N}) \quad (2.1)
\]

where

\[
u_{2i} = \frac{(3i+1)}{2} \quad \text{(for} \ i = 0, 1, \ldots), \quad \nu_{2i-1} = \frac{(3i-1)}{2} \quad \text{(for} \ i = 1, 2, \ldots)
\]

and

\[
\varepsilon_{2i} = \varepsilon_{2i-1} = (-1)^i.
\]

Consider the set

\[
\mathcal{M}_n = \{ n-u_j; 0 \leq u_j \leq n \}. \quad (2.2)
\]

It follows from (2.1) that

\[
\sum_{m \in \mathcal{M}_n} p(m) \equiv 0 \quad \text{(mod} \ 2)
\]
whence
\[\{m : m \in \mathcal{M}_n, \, p(m) \equiv 1 \pmod{2}\} \equiv 0 \pmod{2}. \tag{2.3}\]

Thus if $|\mathcal{M}_n|$ is odd, then there is at least one $m \in \mathcal{M}_n$ for which $p(m)$ is even.

If $k$ is definite by $u_{k-1} \leq n < u_k$, then we have $|\mathcal{M}_n| = k$. Thus $|\mathcal{M}_n|$ is odd if and only if $n$ is in an interval of type
\[\left[u_{2j}, u_{2j+1}\right) = \left[\frac{j(3j+1)}{2}, \frac{(j+1)(3j+3)}{2}\right).\]

For some $n \in \mathbb{N}$, the total length of intervals of this type contained in $\{1, N\}$ is $c_5N$ (indeed, their total length is $(2/3 + o(1)) N$). Thus we have
\[\{|(m, n) : m \in \mathcal{M}_n, \, p(m) \equiv 0 \pmod{2}\}| > c_4N.\]

A number $m$ is counted for those values of $n$ that are of the form $n = m + u_j$. For $m$ fixed, the number of such integers $n$ is at most the number of $j$'s satisfying $u_j \leq N$ which is, clearly, $\leq c_5N^{1/2}$. Thus there at least $c_4N/c_5N^{1/2} = c_4N^{1/2}$ distinct values of $m$ for which $p(m)$ is even and this completes the proof of Theorem 1.

3

Proof of Theorem 2. Write $f(n) = p(n) - p(n - 1)$. By (2.1) we have
\[\sum_{j=0}^{+\infty} a_j f(n-u_j) = 0 \quad \text{for all } n \in \mathbb{N}.\]

Again, define $\mathcal{M}_n$ by (2.2). Then as in (2.3) we have
\[\{m : m \in \mathcal{M}_n, \, f(m) \equiv 1 \pmod{2}\} \equiv 0 \pmod{2}. \tag{3.1}\]

Consider now an integer $n$ of the form $n = u_k$. Then the number $m = 0 = n - u_k$ is counted in (3.1) since we have
\[f(0) = 1 \equiv 1 \pmod{2}.\]

But then, by (3.1), the set $\{m : m \in \mathcal{M}_n, \, f(m) \equiv 1 \pmod{2}\}$ must have at least one further element. Thus for any $k \in \mathbb{N}$, $k \geq 2$ there is an integer $j$ such that $0 \leq j \leq k - 1$ and, taking $m = u_k - u_j$, the number $p(m) = p(u_k - u_j)$ is odd.
There are at least \( c_7 N^{1/2} \) numbers \( u_k \) with \( u_k \leq N \), and to each of these numbers \( u_k \), we assign a number \( m \leq N \). Now we will estimate the multiplicity of these numbers \( m \). To do this, observe that the numbers \( u_k \) are of the form
\[
u_k = \frac{t(3t+1)}{2}
\]
where \( t = i \) if \( k = 2i \), and \( t = -i \) if \( k = 2i - 1 \). Thus \( m = u_k - u_j \) is of the form
\[
m = u_k - u_j = \frac{t(3t+1)}{2} - \frac{s(3s+1)}{2} = \frac{(t-s)(3t+3s+1)}{2} \tag{3.2}
\]
with certain integers \( t, s \). Here \( t - s \) is a (positive or negative) divisor of \( m \), thus the total number of possible values of \( t - s \) is at most \( 2\tau(m) \) (where \( \tau(m) \) is the divisor function). If \( t - s \) is given then it follows from (3.2) that
\[
\begin{align*}
t + s &= \frac{1}{3} \left( \frac{2m}{t-s} - 1 \right)
\end{align*}
\]
and \( t - s \) and \( t + s \) determine \( t \) and \( s \), and thus also \( k \) and \( j \) uniquely. We may conclude that the number \( m \) is counted with multiplicity at most \( 2\tau(m) \) which is, by Wigert’s theorem \([12]\),
\[
2\tau(m) \leq 2 \max_{m \leq N} \tau(m) < \exp \left( (\log 2 + \varepsilon/2) \frac{\log N}{\log \log N} \right) \quad \text{(for } N > N_3(\varepsilon))
\]
Thus the total number of the distinct \( m \) values counted is at least
\[
c_7 N^{1/2} \exp \left( (\log 2 + \varepsilon/2) \frac{\log N}{\log \log N} \right)
\]
\[
> N^{1/2} \exp \left( -(\log 2 + \varepsilon) \frac{\log N}{\log \log N} \right) \quad \text{(for } N > N_4(\varepsilon))
\]
which completes the proof of Theorem 2.

4

Proof of Theorem 4. The set \( \mathcal{A} \) of the desired properties will be defined by recursion. We write \( \mathcal{A}_n = \mathcal{A} \cap \{1, 2, ..., n\} \). Let
\[
A_3 = \{1, 2, 3\}.
\]
Assume that \( n \geq 4 \) and \( \mathcal{A}_{n-1} \) has been defined so that \( p(\mathcal{A}, m) \) is even for \( 4 \leq m \leq n-1 \). Then set
\[
A \in \mathcal{A} \quad \text{if and only if} \quad p(\mathcal{A}_{n-1}, n) \quad \text{is odd.} \tag{4.1}
\]
Note that \( p(\mathcal{A}_4, 4) = 4 \), so that \( 4 \notin \mathcal{A}_4 \). We will show that the set \( \mathcal{A} = \{1, 2, 3, 5, 8, 9, 10, 13, 14, 16, \ldots \} \) obtained in this way satisfies (1.1) and (1.2).

It follows from the construction that for \( n \geq 4 \) we have
\[
\begin{align*}
&\text{if}\ n \in \mathcal{A},\quad p(\mathcal{A}, n) = 1 + p(\mathcal{A}_{n-1}, n) \\
&\text{if}\ n \notin \mathcal{A},\quad p(\mathcal{A}, n) = p(\mathcal{A}_{n-1}, n)
\end{align*}
\]
which, with (4.1), proves (1.1).

(Note that in the same way, any finite set \( \mathcal{B} = \{b_1, b_2, \ldots, b_k\} \) can be extended to an infinite set \( \mathcal{A} \) so that \( \mathcal{A}_k = \mathcal{B} \) and the parity of \( p(\mathcal{A}, b_k + 1)\), \( p(\mathcal{A}, b_k + 2)\), \ldots is given. The difficulty is the estimate of \( A(x) \).)

Next we will prove (1.2). Write
\[
\sigma(\mathcal{A}, n) = \sum_{d \mid n, d \in \mathcal{A}} d
\]
and
\[
f(\mathcal{A}, x) = \sum_{n=0}^{\infty} p(\mathcal{A}, n) x^n;
\]
by
\[
p(\mathcal{A}, n) \leq p(N, n) = \exp(o(n)),
\]
this power series is absolutely convergent for \( |x| < 1 \). Moreover, by the definition of \( p(\mathcal{A}, n) \) for \( |x| < 1 \) we have
\[
f(\mathcal{A}, x) = \prod_{a \in \mathcal{A}} \left( \sum_{k=0}^{\infty} x^{ka} \right) = \prod_{a \in \mathcal{A}} \frac{1}{1-x^a}.
\]
Taking the logarithmic derivative of both sides we obtain for \( |x| < 1 \) that
\[
\frac{f'(\mathcal{A}, x)}{f(\mathcal{A}, x)} = \sum_{a \in \mathcal{A}} \frac{ax^{a-1}}{1-x^a}
\]
whence
\[
xf'(\mathcal{A}, x) = f(\mathcal{A}, x) \sum_{a \in \mathcal{A}} \frac{ax^a}{1-x^a}. \tag{4.2}
\]
Here we have

$$xf'(.A, x) = \sum_{n=1}^{+\infty} np(.A, n) x^n$$  \hspace{1cm} (4.3)

and

$$f(.A, x) \sum_{a \in .A} \frac{ax^a}{1-x} = f(.A, x) \sum_{a \in .A} \sum_{k=1}^{+\infty} ax^{ak}$$

$$= f(.A, x) \left( \sum_{n=1}^{+\infty} \left( \sum_{a | n, a \in .A} a \right) x^n \right)$$

$$= \sum_{n=0}^{+\infty} p(.A, n) x^n \sum_{n=1}^{+\infty} \sigma(.A, n) x^n$$

$$= \sum_{n=1}^{+\infty} \left( \sum_{k=0}^{n-1} p(.A, k) \sigma(.A, n-k) \right) x^n. \hspace{1cm} (4.4)$$

It follows from (4.2), (4.3) and (4.4) that

$$np(.A, n) = \sum_{k=0}^{n-1} p(.A, k) \sigma(.A, n-k) \hspace{1cm} \text{(for } n = 1, 2, \ldots). \hspace{1cm} (4.5)$$

(This identity generalizes the well-known recursive formula

$$np(n) = \sum_{k=0}^{n-1} p(k) \sigma(n-k)$$

for $p(n).$)

By (1.1), it follows from (4.5) that for $n \geq 4$ we have

$$0 \equiv np(.A, n)$$

$$\equiv \sigma(.A, n) + p(.A, 1) \sigma(.A, n-1) + p(.A, 2) \sigma(.A, n-2)$$

$$+ p(.A, 3) \sigma(.A, n-3)$$

$$\equiv \sigma(.A, n) + \sigma(.A, n-1) + \sigma(.A, n-3) \hspace{1cm} \text{(mod } 2)$$

whence

$$\sigma(.A, n) \equiv \sigma(.A, n-1) + \sigma(.A, n-3) \hspace{1cm} \text{(mod } 2) \hspace{1cm} \text{(for } n \geq 4). \hspace{1cm} (4.6)$$
A simple computation gives that

\[
\sigma(\mathcal{A}, 1) = 1 \equiv 1 \pmod{2}, \quad \sigma(\mathcal{A}, 2) = 3 \equiv 1 \pmod{2} \quad \text{and} \\
\sigma(\mathcal{A}, 3) = 4 \equiv 0 \pmod{2}.
\] (4.7)

Combining (4.6) with (4.7), we obtain by an easy computation that

\[
\sigma(\mathcal{A}, 4) \equiv 1 \pmod{2}, \quad \sigma(\mathcal{A}, 5) \equiv 0 \pmod{2}, \\
\sigma(\mathcal{A}, 6) \equiv 0 \pmod{2}, \quad \sigma(\mathcal{A}, 7) \equiv 1 \pmod{2}, \\
\sigma(\mathcal{A}, 8) \equiv 1 \pmod{2}, \quad \sigma(\mathcal{A}, 9) \equiv 1 \pmod{2},
\] (4.8)

and

\[
\sigma(\mathcal{A}, 10) \equiv 0 \pmod{2},
\]

so that

\[
\sigma(\mathcal{A}, n + 7) \equiv \sigma(\mathcal{A}, n) \pmod{2} \quad \text{for} \quad n = 1, 2, 3.
\] (4.9)

It follows from (4.6) and (4.9) that

\[
\sigma(\mathcal{A}, n + 7) \equiv \sigma(\mathcal{A}, n) \pmod{2} \quad \text{for all} \quad n \in \mathbb{N}.
\] (4.10)

By (4.7), (4.8) and (4.10), for \( k = 0, 1, 2, \ldots \) we have

\[
\sigma(\mathcal{A}, 7k + i) \equiv \begin{cases} 0 \pmod{2} & \text{if} \quad i = 3, 5, 6 \\ 1 \pmod{2} & \text{if} \quad i = 1, 2, 4. \end{cases}
\] (4.11)

On the other hand, if \( p \) is a prime with \( p > 2 \) then clearly we have

\[
\sigma(\mathcal{A}, p) = \sum_{\substack{a \in \mathcal{A} \mid p \equiv a \pmod{2}}} a = \begin{cases} 1 & \text{if} \quad p \not\equiv \mathcal{A} \\ 1 + p \equiv 0 \pmod{2} & \text{if} \quad p \equiv \mathcal{A}. \end{cases}
\] (4.12)

It follows from (4.11) and (4.12) that if \( p \) is a prime with \( (p, 14) = 1 \) then

\[
p \in \mathcal{A} \quad \text{if} \quad p \equiv 3, 5 \text{ or } 6 \pmod{7}
\]

and

\[
p \not\in \mathcal{A} \quad \text{if} \quad p \equiv 1, 2 \text{ or } 4 \pmod{7}.
\]
Thus by the prime number theorem of the arithmetic progressions of small moduli, for \( x \to +\infty \) we have

\[
A(x) \geqslant \left| \left\{ p: p \text{ prime, } p \leqslant x, \ p \equiv 3, 5 \text{ or } 6 \mod 7 \right\} \right|
\]

\[
= \left( 1 - \frac{1}{2} + o(1) \right) \frac{x}{\log x}
\]  
(4.13)

and

\[
A(x) \leqslant \left[ x \right] - \left\{ \left\{ p: p \text{ prime, } p \leqslant x, \ p \equiv 1, 2 \text{ or } 4 \mod 7 \right\} \right|\]

\[
= x - \left( 1 + o(1) \right) \frac{x}{\log x}
\]  
(4.14)

(1.2) follows from (4.13) and this completes the proof of Theorem 4.

First we thought that, perhaps, even

\[ A(x) = \left( \frac{1}{2} + o(1) \right) x \]

holds. However, computing the elements of \( \mathcal{A} \) up to 10,000, it turned out that \( A(10,000) = 2,204 \) so that, probably,

\[
\liminf_{x \to +\infty} \frac{A(x)}{x} < \frac{1}{2}.
\]

5

Proof of Theorem 5. Assume that contrary to the assertion of the theorem, \( \mathcal{A} \) is an infinite set of positive integers such that (1.5) holds for some \( n_0 \), however, we have

\[
\limsup_{x \to +\infty} \frac{A(x)(\log \log x)^3/2}{(\log x)^{3/2}} < \frac{1}{20}.
\]  
(5.1)

Denote the least integer \( a \) with \( a \in \mathcal{A} \), \( a > n_0 \) by \( a_0 \). Then first we will show that we have

\[
(x, 2x] \cap \mathcal{A} \neq \emptyset \quad \text{for} \quad x > a_0.
\]  
(5.2)

Indeed, assume that contrary to (5.2) there is a real number \( x \) such that

\[
(x, 2x] \cap \mathcal{A} = \emptyset
\]  
(5.3)
and
\[ x > a_0. \]  
(5.4)

Let \( \bar{a} \) denote the greatest element of \( \mathcal{A} \) with \( \bar{a} \leq x \). Then by (5.4) and the definition of \( a_0 \) we have
\[ \bar{a} \geq a_0 > n_0. \]  
(5.5)

Moreover
\[ \bar{a} + \bar{a} = 2\bar{a} \]
is a representation of \( n = 2\bar{a} \) in form \( a + a' = n \) with \( a \in \mathcal{A}, \ a' \in \mathcal{A} \), and this is the only representation of \( 2\bar{a} \) in this form since if \( a \in \mathcal{A}, \ a' \in \mathcal{A} \), then by (5.3) and the definition of \( \bar{a} \) for \( \max(a, a') > \bar{a} \) we have
\[ a + a' \geq \max(a, a') > 2x \geq 2\bar{a} \]
while for \( \max(a, a') \leq \bar{a} \) we have
\[ a + a' < 2\bar{a} \]
unless \( a = a' = \bar{a} \). Thus we have
\[ r(\mathcal{A}, 2\bar{a}) = 1. \]  
(5.6)

(5.5) and (5.6) contradict (1.5) and this completes the proof of (5.2).

Now define the infinite sequence \( \mathcal{B} = \{b_1, b_2, \ldots \} \) (where \( b_1 < b_2 < \cdots \) ) of positive integers by the following recursion:

Let \( b_1 \) denote the smallest element of \( \mathcal{A} \) greater than \( 10^{10} \), so that
\[ b_1 \in \mathcal{A}, \quad b_1 > 10^{10}. \]

Assume now that \( b_1, b_2, \ldots, b_k \) have been defined. Then it follows from (5.1) that there is at least one integer \( b \) such that
\[ b > b_k, \quad [b - b_k, b] \cap \mathcal{A} = b \]
(since otherwise \( \mathcal{A} \) had positive upper density contrary to (5.1)). Let \( b_{k+1} \) denote the smallest of these integers \( b \):
\[ b_{k+1} = \min\{b; b > b_k, [b - b_k, b - 1] \cap \mathcal{A} = \emptyset, b \in \mathcal{A}\}. \]  
(5.7)

Next we will prove
Lemma 1. There is a number $x_1$ such that for $x > x_1$ we have
\[ B(x) > \frac{\log x}{2 \log \log x} \quad \text{(for } x > x_1). \] (5.8)

Proof of Lemma 1. First we will prove that there is a number $k_0$ such that
\[ b_{k+1} < b_k \left( \frac{\log b_k}{\log \log b_k} \right)^{3/2} \quad \text{for } k > k_0. \] (5.9)
Assume that contrary to (5.9), we have
\[ b_{k+1} \geq b_k \left( \frac{\log b_k}{\log \log b_k} \right)^{3/2} \] (5.10)
for a large $k$. We have to show that this indirect assumption leads to a contradiction for every large $k$.

If $k$ is large enough, then by (5.2) there is a number $a$ such that
\[ a \in \left[ \frac{1}{2} b_k \left( \frac{\log b_k}{\log \log b_k} \right)^{3/2}, b_k \left( \frac{\log b_k}{\log \log b_k} \right)^{3/2} \right] \] (5.11)
so that, by (5.10), $A < B_{k+1}$. It follows from (5.10), (5.11) and definition (6.7) of $b_{k+1}$ that
\[ (a - j b_k, a - (j - 1) b_k) \cap \mathcal{A} \neq \emptyset \] (5.12)
for every $j \in \mathbb{N}$ such that
\[ a - j b_k \geq b_k \]

or, in equivalent form,
\[ j + 1 \leq \frac{a}{b_k}, \quad j \leq \left[ \frac{a}{b_k} \right] - 1. \] (5.13)

Writing $y = b_k (\log b_k / \log \log b_k)^{3/2}$, by (5.11), (5.12) and (5.13) for large enough $k$ we have
\[ A(y) \geq A(a) \geq \sum_{j=1}^{[a/b_k] - 1} (A(a - (j - 1)b_k) - A(a - j b_k)) \geq \sum_{j=1}^{[a/b_k] - 1} 1 \\
= \left[ \frac{a}{b_k} \right] - 1 \geq \left[ \frac{1}{2} \left( \frac{\log b_k}{\log \log b_k} \right)^{3/2} \right] - 1 \geq \frac{1}{3} \left( \frac{\log b_k}{\log \log b_k} \right)^{3/2} \]
\[ > \frac{1}{4} \left( \frac{\log y}{\log \log y} \right)^{3/2}. \]
For \( k \) large enough (note that \( y > b_k \)) this contradicts (5.1), and this completes the proof of (5.9).

It remains to derive (5.8) from (5.9). Assume that \( x \) is large, and define the positive integer \( k \) by

\[
b_k \leq x < b_{k+1}.
\]

(5.14)

Then for \( x \) large enough, by (5.9) and (5.14) we have

\[
x < b_{k+1} = b_1 \prod_{k=2}^{k+1} b_{i-1} < O(1) \prod_{i=k_2+2}^{k+1} \left( \frac{\log b_{i-1}}{\log \log b_{i-1}} \right)^{3/2}
\]

\[
\leq \left( \frac{\log b_k}{\log \log b_k} \right)^{3/2} \leq \left( \frac{\log x}{\log \log x} \right)^{3/2}.
\]

whence, for \( x \) large enough,

\[
k > \frac{\log x}{2 \log \log x}.
\]

(5.15)

By (5.14) and (5.15) we have

\[
B(x) \geq B(b_k) = k > \frac{\log x}{2 \log \log x}
\]

which completes the proof of Lemma 1.

Next we will prove

**Lemma 2.** If \( \mathcal{A} \) is defined as above (in particular, (1.5) and (5.1) hold) then there is a positive real number \( x_2 \) such that writing \( z = z(x) = 2x(\log x / \log \log x)^{3/2} \), for \( x > x_2 \) we have

\[
A(z) - A(x) > \frac{1}{3} \left( \frac{\log x}{\log \log x} \right)^{1/2}.
\]

(5.16)

**Proof of Lemma 2.** If \( x \) is large enough then by (5.2) we have

\[
(2x, z/2] \cap \mathcal{A} \neq \emptyset.
\]

(5.17)

Let \( \mathcal{A} = \{a_1, a_2, \ldots\} \) with \( a_1 < a_2 < \cdots \), and define \( M_x \) by

\[
M_x = \max_{2x < a_i < z/2} (a_i - a_{i-1}).
\]

(5.18)

(The set \( 2x < a_i < z/2 \) is non-empty by (5.17).)
Case 1. Assume first that 
\[ M_x \leq x. \] (5.19)

By (5.2), for \( x \) large enough there is an integer \( a' \) with 
\[ \frac{z}{4} < a' \leq \frac{z}{2}, \quad a' \in \mathcal{A}. \] (5.20)

Then by (5.20) and the definition of \( M_x \), for every positive integer \( j \) with 
\[ a' - jx > x \] (5.21)
we have 
\[ \{a' - jx, a' - (j - 1)x\} \cap \mathcal{A} \neq \emptyset. \] (5.22)

(5.21) can be rewritten in the equivalent form 
\[ j < \frac{a'}{x} - 1. \] (5.23)

By (5.20), (5.23) follows from 
\[ j < \frac{z}{4x} - 1. \]

Thus by (5.20) and (5.22), for \( x \) large enough we have 
\[ A(z) - A(x) \geq A(a') - A(x) \geq \sum_{j=1}^{[z/4x]} (A(a' - (j - 1)x) - A(a' - jx)) \geq \sum_{j=1}^{[z/4x]} 1 \]
\[ = \left[ \frac{z}{4x} \right] - 2 > \frac{z}{5x} \geq \frac{1}{3} \left( \frac{\log x}{\log \log x} \right)^{3/2} \]
so that (5.16) holds in this case.

Case 2. Assume now that 
\[ M_x > x. \] (5.24)

Assume that the maximum in (5.18) is attained for \( i = i_0 \):
\[ M_x = a_{i_0} - a_{i_0 - 1}, \]
and write $a_i = a^\ast$. Consider all the sums

$$b_i + a^\ast \quad \text{with} \quad i = 1, 2, \ldots, B(x).$$

Here we have $b_i \in \mathcal{B} \subset \mathcal{A}$ so that

$$r(\mathcal{A}, b_i + a^\ast) \geq 1 \quad \text{for} \quad i = 1, 2, \ldots, B(x).$$

By (1.5) and

$$b_i + a^\ast > a^\ast > 2x, \quad (5.25)$$

this implies for $x$ large enough that

$$r(\mathcal{A}, b_i + a^\ast) \geq 2 \quad \text{for} \quad i = 1, 2, \ldots, B(x),$$

so that each of the numbers $b_i + a^\ast$ must have at least one further representation in form $a' + a''$ with $a' \in \mathcal{A}$, $a'' \in \mathcal{A}$. Let

$$b_i + a^\ast = a'_i + a''_i \quad (\text{for} \quad i = 1, 2, \ldots, B(x)) \quad (5.26)$$

with

$$a'_i \in \mathcal{A}, \quad a''_i \in \mathcal{A}, \quad a'_i \leq a''_i \quad (5.27)$$

and

$$\max(b_i, a^\ast) \neq a''_i. \quad (5.28)$$

For $1 \leq i \leq B(x)$ clearly we have

$$b_i \leq b_{B(x)} \leq x$$

so that by (5.25), (5.28) can be replaced by

$$a^\ast \neq a''_i.$$

Let $\mathcal{I}_1$ denote the set of the integers $i$ with $1 \leq i \leq B(x)$ and $a''_i < a^\ast$ so that

$$a''_i < a^\ast \quad (\text{for} \quad i \in \mathcal{I}_1). \quad (5.29)$$

and write $\mathcal{I}_2 = \{1, 2, \ldots, B(x)\} \setminus \mathcal{I}_1$ (so that $a''_i > a^\ast$ for $i \in \mathcal{I}_2$).

If $i \in \mathcal{I}_1$ then by (5.24), (5.26), (5.29) and the definition of $a^\ast$ we have

$$a'_i = a^\ast + b_i - a''_i > a^\ast - a''_i = a_0 - a''_i \geq a_0 - a_{0-1} = M > x. \quad (5.30)$$
It follows from (5.27), (5.29), (5.30) and
\[ a^* = a_{i_0} < z/2 < z \tag{5.31} \]
that \( a'_i \in \mathcal{A}, \; a^*_i \in \mathcal{A} \) and
\[ x < a'_i \leq a^*_i < a^* < z. \tag{5.32} \]
Clearly, the number of pairs \((a'_i, a^*_i)\) with these properties is at most
\((A(z) - A(x))^2\) so that
\[ |I_1| \leq (A(z) - A(x))^2. \tag{5.33} \]
Assume now that
\[ |I_2| \geq 2, \]
and let \( i \in I_2, \; j \in I_2, \; i < j \) \((\leq B(x))\). Then by the definition of \( I_2 \) we have
\[ a^*_i > a^*, \quad a^*_j > a^*. \tag{5.34} \]
Now we will show that
\[ a^*_i < a^*_j. \tag{5.35} \]
We will prove this by showing that the opposite inequality
\[ a^*_i \geq a^*_j \tag{5.36} \]
leads to a contradiction.

By (5.26) we have
\[ a^*_i = a^* + b_j - a'_i < a^* + b_j. \tag{5.37} \]
It follows from (5.26) (with \( j \) in place of \( i \)), (5.36) and (5.37) that
\[ a'_j = a^* + b_j - a^*_i \geq a^* + b_j - a^*_i > a^* + b_j - (a^* + b_j) \]
\[ = b_j - b_{j-1} \geq b_j - b_{j-1}. \tag{5.38} \]
On the other hand, by (5.26) (with \( j \) in place of \( i \)) and (5.34) we have
\[ a'_j = a^* + b_j - a^*_j < a^* + b_j - a^* = b_j. \tag{5.39} \]
It follows from (5.38) and (5.39) that
\[ [b_j - b_{j-1}, b_j) \cap \mathcal{A} \neq \emptyset \]
which contradicts definition (5.7) of \( b_j \), and this proves (5.35).
Thus if we write $|\mathcal{S}_2| = t$ and $\mathcal{S}_2 = \{i_1, i_2, \ldots, i_t\}$ where $i_1 < i_2 < \cdots < i_t$, and $t \geq 2$, then by (5.34), (5.35) and (5.37) we have
\[ a^* < a_1^* < a_2^* < \cdots < a_t^* < a^* + b \leq a^* + b \mathcal{B}(x) \leq a^* + x. \quad (5.40) \]

It follows from (5.25), (5.31) and (5.40) that
\[ x < a_1^* < a_2^* < \cdots < a_t^* < a^* + x \leq \frac{x}{2} + x < z \]
where $a_1^* \in \mathcal{A}, \ldots, a_t^* \in \mathcal{A}$. Thus $|\mathcal{S}_2| = t \geq 2$ implies
\[ |\mathcal{S}_2| = t \leq |\{a : x < a < z, a \in \mathcal{A}\}| \leq A(z) - A(x) \]
so that
\[ |\mathcal{S}_2| \leq (A(z) - A(x)) + 1. \quad (5.41) \]

It follows from (5.33), (5.41) and the definition of $\mathcal{S}_1$ and $\mathcal{S}_2$ that
\[ \mathcal{B}(x) = |\mathcal{S}_1| + |\mathcal{S}_2| \leq (A(z) - A(x))^2 + (A(z) - A(x)) + 1 \]
\[ \leq 2(A(z) - A(x))^2 + 1. \]

By Lemma 1, this implies that
\[ A(z) - A(x) \geq \left( \frac{1}{2} \mathcal{B}(x) - 1 \right)^{1/2} \geq \frac{1}{3} \left( \frac{\log x}{\log \log x} \right)^{1/2} \]
so that (5.16) holds also in Case 2 and this completes the proof of Lemma 2.

Completion of the Proof of Theorem 5. It remains to derive a contradiction with (1.6) from Lemma 2.

Let $x$ be a large number, and define the numbers $y_0 > y_1 > \cdots > y_u$ with $u = u(x)$ in the following way: let $y_0 = x$,
\[ y_{j-1} = 2y_j \left( \frac{\log y_j}{\log \log y_j} \right)^{3/2} \quad \text{for} \quad j = 1, 2, \ldots, \]
and define the positive integer $u$ by
\[ y_{u-1} \geq x^{1/2} > y_u. \quad (5.42) \]
Then we have
\[
\frac{x^{1/2}}{y_u/n} = \prod_{j=1}^{u} \frac{y_{j-1}}{y_j} = \prod_{j=1}^{u} \frac{y_j}{y_{j+1}} = \frac{2}{2} \left( \frac{\log y_j}{\log \log y_j} \right)^{1/2} < \left( \frac{2}{2} \right) \left( \frac{\log x}{\log \log x} \right)^{1/2}.
\]
For \( x \) large enough it follows that
\[
u > \frac{1}{4} \frac{\log x}{\log \log x}.
\]
By (5.42), (5.43) and Lemma 2, we have
\[
A(x) \geq A(x) - A(y_i) = \sum_{j=1}^{u} \left( A(y_{j-1}) - A(y_j) \right) > \sum_{j=1}^{u} \frac{1}{3} \left( \frac{\log y_j}{\log \log y_j} \right)^{1/2} \geq \frac{1}{3} \left( \frac{\log y_{u-1}}{\log \log y_{u-1}} \right)^{1/2} \geq \frac{1}{5} \left( \frac{\log x}{\log \log x} \right)\]
\[
> \frac{1}{20} \left( \frac{\log x}{\log \log x} \right)^{1/2}
\]
for all \( x \) large enough which contradicts (5.1) and this completes the proof of Theorem 5.

6

Proof of Theorem 6. For \( n \in \mathbb{N} \), let \( g(n) \) denote the number of 2-powers used in the binary representation of \( n \), i.e., if
\[
n = \sum_{i=0}^{t} e_i 2^i \quad \text{with} \quad e_i = 0 \text{ or } 1 \quad \text{(for } i = 0, 1, \ldots, t),
\]
then let
\[
g(n) = \sum_{i=0}^{t} e_i.
\]
Define the set \( \mathcal{A} \) by
\[
\mathcal{A} = \{ n : n \in \mathbb{N}, g(n) = 1 \text{ or } 2 \}.
\]
We will show that this set \( \mathcal{A} \) has the desired properties.
In order to show (1.7), observe that if \( n \not\in \mathcal{A}, n \leq x \) then
\[
\{ 2^n : u \in \mathbb{Z}, 0 \leq u, 2^n \leq x \} \cup \{ 2^n + 2^v : u, v \in \mathbb{Z}, 0 \leq u < v, 2^v \leq x \}.
\]
Clearly we have
\[
\left| \{ 2^n : u \in \mathbb{Z}, 0 \leq u, 2^n \leq x \} \right| = \left\lfloor \frac{\log x}{\log 2} \right\rfloor + 1
\]
and
\[
\left| \{ 2^n + 2^v : u, v \in \mathbb{Z}, 0 \leq u < v, 2^v \leq x \} \right|
\leq \left( \left\lfloor \frac{\log x}{\log 2} \right\rfloor + 1 \right) \left( \left\lfloor \frac{\log x}{\log 2} \right\rfloor + 1 \right)
\leq \frac{(\log x)^2}{\log 2}.
\]
It follows that
\[
A(x) \leq \left\lfloor \frac{\log x}{\log 2} \right\rfloor + 1 + \frac{(\log x)^2}{\log 2}
\]
whence
\[
\limsup_{x \to +\infty} A(x)(\log x)^{-2} \leq (\log 2)^{-2}
\]
which proves (1.7).

In order to prove (1.8) first we prove

**Lemma 3.** If \( n \in \mathbb{N} \) and \( n \) is the sum of \( t \) 2-powers, i.e.,
\[
n = 2^i_1 + 2^i_2 + \ldots + 2^i_t \quad (6.1)
\]
where \( t \in \mathbb{N}, i_1, i_2, \ldots, i_t \in \mathbb{Z}, \) and \( 0 \leq i_1 \leq i_2 \leq \ldots \leq i_t, \) then we have
\[
g(n) \leq t. \quad (6.2)
\]

**Proof of Lemma 3.** We prove the assertion of the lemma by induction on \( t. \) If \( t = 1 \) then (6.2) holds trivially with equality sign. Assume now that \( t \geq 2 \) and (6.2) holds with \( t-1 \) in place of \( t. \) Consider now a positive integer \( n \) of the form (6.1). If \( i_j \leq i_j + \) for each of \( j = 1, 2, \ldots, t-1, \) then again (6.2) holds with equality sign. If there is a \( j \) with \( i_j = i_{j+1}, \) then replacing \( 2^i_j + 2^i_{j+1} \) by \( 2^{i_j+1} \) on the right hand side of (6.1) we obtain the representation of \( n \) as the sum of \( t-1 \) 2-powers, and thus by our induction
hypothesis we have $g(n) \leq t - 1$ which implies (6.2), and this completes the proof of Lemma 3.

It follows trivially from Lemma 3 that
\[ g(u + v) \leq g(u) + g(v) \quad \text{for all } u, v \in \mathbb{N}. \]

Consequently, if $n$ can be represented in the form $n = a + a'$ with $a, a' \in \mathcal{A}$ then we have
\[ g(n) \leq g(a) + g(a') \leq 2 + 2 = 4. \]

Thus to prove (1.8), it suffices to show that if
\[ g(n) \leq 4 \]
and
\[ n \geq 4, \tag{6.3} \]
then $r(\mathcal{A}, n) \geq 2$, i.e., $n$ has at least two representations in the form
\[ n = a + a' \quad \text{with } a \leq a' \tag{6.4} \]
and $a, a' \in \mathcal{A}$, i.e.,
\[ 1 \leq g(a), \quad g(a') \leq 2. \tag{6.5} \]

To show this, we have to distinguish four cases.

Case 1. Assume first that $g(n) = 4$, i.e.,
\[ n = 2^u + 2^v + 2^z + 2^w \quad \text{with } u < v < z < w. \]
Then choosing first $a = 2^u + 2^v$, $a' = 2^v + 2^w$ and then $a = 2^u + 2^z$, $a' = 2^z + 2^w$, we obtain two different representations of $n$ satisfying (6.4) and (6.5).

Case 2. Assume now that $g(n) = 3$, i.e.,
\[ n = 2^u + 2^v + 2^z \quad \text{with } u < v < z. \]
Then clearly $2^z + (2^v + 2^z)$ and $(2^v + 2^z) + 2^z$ are two different representations of $n$ in the form (6.4) with $a, a' \in \mathcal{A}$ and (6.5).

Case 3. Assume that $g(n) = 2$, i.e.,
\[ n = 2^u + 2^v \quad \text{with } u < v. \]
Then (6.4) and (6.5) hold with $a = 2^u$ and $a' = 2^v$, so that it suffices to find a second representation of $n$ in the form $a + a'$. By (6.3), at least one of the
inequalities \( u \geq 1, v \geq u + 2 \) holds. In the first case \( a = 2^{u-1}, \ a' = 2^{u-1} + 2^v \), while in the second case \( a = 2^{v-1}, \ a' = 2^v + 2^{v-1} \) provides a second representation of the desired form.

Case 4. Assume finally that \( g(n) = 1 \), i.e., \( n = 2^u \). Then by (6.3), the pairs \( a = 2^{u-1}, \ a' = 2^{u-1}, \) resp. \( a = 2^{v-2}, \ a' = 2^{v-2} + 2^{v-1} \) provide two different representations of \( n \) in the desired form, and this completes the proof of Theorem 6.

7

Define the sequence \( E = \{e_1, e_2, ...\} \in \{-1, +1\}^\infty \) in the following way: let

\[
    e_n = \begin{cases} 
        +1 & \text{if } p(n) \equiv 1 \pmod{2} \\
        -1 & \text{if } p(n) \equiv 0 \pmod{2}.
    \end{cases} \tag{7.1}
\]

From the computations of Parkin and Shanks ([7]), the study of the parity of \( p(n) \) leads quite naturally to the guess that the binary sequence \( E \) is “of random type”, or, more exactly, it is a “pseudorandom” sequence. However, it seems to be hopeless to prove any strict mathematical theorem in this direction. At the present, even the proof of the weakest “random type” property

\[
    \lim_{N \to \infty} \frac{|\{n: n \leq N, e_n = +1\}|}{|\{n: n \leq N, e_n = -1\}|} = 1
\]

seems to be beyond our reach. Thus the best that we can do is to gather some numerical evidence by testing the finite sequence

\[ E_N = \{e_1, e_2, ..., e_N\} \]

for pseudorandomness for a possibly large \( N \).

As measures of pseudorandomness of finite binary sequences, Mauduit and Szárkozy [3] propose to use the “well-distribution measure” and “correlation measure”. The well-distribution measure and correlation measure of order 2 of the sequence \( E_N = \{e_1, e_2, ..., e_N\} \) with \( e_i = \pm 1 \) are defined as

\[
    W(E_N) = \max_{1 \leq a < a + kb \leq N} |e_a + e_{a+b} + \cdots + e_{a+kb}| \tag{7.2}
\]
and

\[ C_2(E_N) = \max_{1 \leq k \leq N-1} \max_{1 \leq d \leq N-k} \left( \sum_{i=0}^{N-k-d} e_{k+i} e_{k+d+i} \right) \quad (7.3) \]

respectively; if these measures are “much smaller” than \( N \), then the sequence \( E_N \) can be considered to be pseudorandom. (One might light to study (auto)correlation of higher order, too, but this would restrict the size of \( N \) considerably.)

We are pleased to thank Marc Deléglise who has computed these measures for the sequence \( E_n = \{e_1, e_2, \ldots, e_N\} \) (where \( e_N \) is defined by (7.1) and has obtained:

<table>
<thead>
<tr>
<th>( N )</th>
<th>( W(E_N) )</th>
<th>( a ) max</th>
<th>( b ) max</th>
</tr>
</thead>
<tbody>
<tr>
<td>100</td>
<td>16</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>1000</td>
<td>55</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>5000</td>
<td>81</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>12000</td>
<td>91</td>
<td>146</td>
<td>10</td>
</tr>
<tr>
<td>20000</td>
<td>90</td>
<td>6663</td>
<td>13</td>
</tr>
<tr>
<td>100000</td>
<td>641</td>
<td>21017</td>
<td>1</td>
</tr>
</tbody>
</table>

where \( a \) max and \( b \) max give one value of \( a \) and \( b \) for which the maximum in (7.2) is attained. For \( C_2(E_N) \) M. Deléglise has found:

<table>
<thead>
<tr>
<th>( N )</th>
<th>( C_2(E_N) )</th>
<th>( k ) max</th>
<th>( d ) max</th>
</tr>
</thead>
<tbody>
<tr>
<td>100</td>
<td>20</td>
<td>2</td>
<td>20</td>
</tr>
<tr>
<td>1000</td>
<td>85</td>
<td>69</td>
<td>74</td>
</tr>
<tr>
<td>10000</td>
<td>374</td>
<td>2501</td>
<td>451</td>
</tr>
</tbody>
</table>

where \( k \) max and \( d \) max give a value of \( k \) and \( d \) for which the maximum in (7.3) is attained. The values of \( W(E_N) \) and \( C_2(E_N) \) displayed above are much smaller than \( N \), so that, indeed, one expects the infinite sequence \( E \) to be pseudorandom.

APPENDIX

J.-P. Serre

Le Théorème 3 ci-dessus peut être généralisé de la façon suivante:
Soit \( f = \sum a_n q^n \) une série à coefficients (mod 2), que je suppose “modulaire” (au sens précis ci-dessous), de poids entier (positif ou négatif, mais c'est

1 Collège de France, 3 rue d’Ulm, F-75231 Paris cedex 05, France. E-mail: serre@dmi.ens.fr.
le cas négatif qui nous intéresse). Soit $L$ une progression arithmétique. Notons $Z_{L,f}(N)$ le nombre des entiers $n \in L$ avec $0 < n \leq N$ tels que $a_n = 0$.

**Théorème.** On a $Z_{L,f}(N)/N^{1/2} \to \infty$ pour $N \to \infty$.

Voici ce que j'entends par “modulaire”: réduction mod 2 d'une fonction modulaire de poids $k$, avec $k \in \mathbb{Z}$, sur un sous-groupe de congruence de $SL_2(\mathbb{Z})$, cette fonction étant holomorphe dans le demi-plan de Poincaré, et méromorphe aux pointes. Une autre façon d'énoncer ces propriétés est de dire qu'il existe une puissance $A^m$ de $A$ (définie par $A(q) = q \prod_{n=1}^{\infty} (1 - q^n)^{2k}$) telle que le produit $f \cdot A^m$ soit une forme modulaire de poids entier $> 0$ sur un groupe de congruence.

Pour appliquer ceci à la fonction de partition, on peut par exemple prendre pour $f$ la fonction

$$f(z) = \eta(3z)^{-1} = \sum_{n=0}^{\infty} p(n) \frac{q^{24n-1}}{q^{24}} \mod 2,$$

qui est de poids $-4$, et le Théorème 3 découle alors du théorème ci-dessus.

**Démonstration du Théorème.** Si $f = \sum a_n q^n$ est une série de Laurent, je note $P_f(N)$ le nombre des entiers $n$, avec $0 < n \leq N$, tels que $a_n \neq 0$. Si $c$ et $a$ sont des nombres réels $\geq 0$, je dirai que

- $f$ est de type $(c, a)$ si $P_f(N) = cN^a(1 + o(1))$ pour $N \to \infty$,
- $f$ est de type $(c, a)^+$ si $P_f(N) \geq cN^a(1 + o(1))$ pour $N \to \infty$,
- $f$ est de type $(c, a)^-$ si $P_f(N) \leq cN^a(1 + o(1))$ pour $N \to \infty$.

**Lemme 0.** Soient $f$ et $f'$ deux séries, et $c'$ un nombre réel $> 0$. Si $ff'$ est de type $(cc', a + a')^+$ et $f'$ de type $(c', a')^-$, alors $f$ est de type $(c, a)^+$.

C'est facile.

Rappelons maintenant que la série $A$ vérifie:

$$A(q) = q \sum_{n=1}^{\infty} (1 - q^n)^{2k} = \sum_{n=0}^{\infty} q^{(2n+1)^2} \mod 2.$$

**Lemme 1.** Si $d$ est un entier $\geq 0$, la série $A^{2d}$ est de type $(c, 1/2)$, avec $c = 2^{-1 - d/2}$.

Si $d = 0$, cela se voit sur la formule ci-dessus. Le cas général se ramène au cas $d = 0$.

**Lemme 2.** La série $A^{2d}(1 + q)$ est de type $(1/2, 1)$. 
De façon plus précise, un calcul élémentaire montre que, si $F$ est cette série, on a $P_F(N) = N/2 + O(N^{1/2})$ pour $N \rightarrow \infty$.

**Lemme 3.** Soient $a$ et $m$ des entiers $\geq 0$, avec $m > 0$. Soit $g = q^a/(1 + q^m)$. La série $f = g \cdot A^{2d}$ est de type $(1/2m, 1)$.

On peut évidemment supposer que $a = 0$. Dans ce cas, si l’on pose $h = 1 + q + \cdots + q^{m-1}$, le produit $fh$ est égal à la série du Lemme 2, donc est de type $(1/2, 1)$. Or $h$ est de type $(m, 0)$. En appliquant le Lemme 0 on en déduit le résultat voulu.

Revenons maintenant à la série $f$ du théorème ci-dessus. Notons $f_L$ la série déduite de $f$ en conservant les termes $a_nq^n$ si $n \in L$, et en les remplaçant par 0 sinon. Un argument modulaire standard montre que $f_L$ vérifie les mêmes hypothèses que $f$: c’est aussi une fonction “modulaire” (sur un sous-groupe de congruence plus petit, mais peu importe). Quitte à remplacer $f$ par $f_L$, on peut donc supposer que $a_n = 0$ si $n \notin L$. Supposons que la progression arithmétique soit formée des entiers $n$ tels que $n \equiv a \pmod m$, et posons $g = q^a/(1 + q^m)$, $h = f + g$. Il est clair que, pour $n \geq a$, on a:

le $n$-ième coeff. de $h$ est $\neq 0 \Leftrightarrow n \in L$ et le $n$-ième coeff. de $f$ est 0.

Tout revient donc à prouver que $h$ est de type $(C, 1/2)$ quelle que soit la constante $C$.

Pour cela, on multiplie l’équation $f + g = h$ par $A^{2d}$, pour $d$ tendant vers l’infini. Si $d$ est assez grand, le produit $f \cdot A^{2d}$ est une forme modulaire de poids $> 0$, donc est lacunaire d’après [9]), c’est-à-dire de type $(\varepsilon, 1)^-$ pour tout $\varepsilon > 0$. D’autre part, le Lemme 3 montre que $g \cdot A^{2d}$ est de type $(1/2m, 1)^+$. Il en résulte que $h \cdot A^{2d}$ est de type $(1/2m - \varepsilon, 1)^+$ pour tout $\varepsilon > 0$. En combinant les Lemmes 0 et 1, on en déduit que $h$ est de type $(C, 1/2)^+$, avec $C = (1/2m - \varepsilon) 2^{1+4\varepsilon}$ pour tout $\varepsilon > 0$ et tout $d$ assez grand. D’où le résultat voulu.

**REFERENCES**


