PUBLICATIONS DE L'INSTITUT MATHÉMATIQUE
Nouvelle série, tome 63 (77), 1998, 21–25

ATKIN'S THEOREM ON PSEUDO-SQUARES

R. Balasubramanian and **D.S. Ramana**

Communicated by Aleksandar Ivić

Abstract. We give an elementary proof of a theorem of A.O.L. Atkin on psuedo-squares. As pointed out by Atkin, from this theorem it immediately follows that there exists an infinite sequence of positive integers, whose j th term $s(j)$ satisfies $s(j) = j^2 + O(\log(j))$, such that the set of integers representable as a sum of two distinct terms of this sequence is of positive asymptotic density.

1. Introduction. In [**1**] Atkin proves the existence of an infinite sequence of positive integers, whose j th term $s(j)$ satisfies $s(j) = j^2 + O(\log(j))$, such that the set of integers representable as a sum of two distinct terms of this sequence is of positive asymptotic density. See also [**2**, Ch. 3, Sec. 2, p. 113]. Atkin deduces this result as an immediate consequence of the following theorem.

Let N and M be positive integers such that M satisfies $a/\log(N) \leq M \leq b/\log(N)$ for some positive real numbers a and b. This assumption will hold throughout.

Let $L(N, M)$ denote the set of mappings from the set $\{1, 2, \ldots, N\}$ into the set of integers in the closed interval $[-M, M]$. For any λ in $L(N, M)$, let $\Im(N, \lambda)$ denote the set $\{(N+1)^2+\lambda(1), \ldots, (N+k)^2+\lambda(k), \ldots, (2N)^2+\lambda(N)\}$. Let $R(N, \lambda)$ denote the number of integers representable as a sum of two *distinct* elements of $\Im(N, \lambda)$.

Theorem. *For sufficiently large N there exists λ in $L(N, M)$ such that $R(N, \lambda) \gg N^2$.*

Using a combinatorial argument, Atkin reduces the proof of this theorem to the estimation of a certain integral. This estimation is then done in [**1**] by the Hardy–Littlewood method.

The purpose of this note is to point out that arranging the combinatorial content of [**1**] differently yields a simple and elementary proof of the above theorem.

AMS Subject Classification (1991): Primary 11B13

2. Proof of the theorem. For any integer k and any λ in $L(N,M)$ let $r(k,\lambda)$ denote the number of ordered pairs (s,t) of distinct elements of the set $\Im(N,\lambda)$ such that $s+t$ is k. Clearly one has

$$\sum_{k\in\mathbf{Z}} r(k,\lambda) = N^2 - N \tag{1}$$

$R(N,\lambda)$ is the number of integers k for which $r(k,\lambda) \neq 0$. Therefore, if the sum $\sum r^2(k,\lambda)$ taken over all integers k, is denoted by $T(N,\lambda)$, the Cauchy–Schwarz inequality gives

$$R(N,\lambda) \geq (N^2-N)^2/T(N,\lambda) \tag{2}$$

Inequality (2) reduces the proof of the theorem to that of Lemma 1.

Lemma 1. *For sufficiently large N there exists λ in $L(N,M)$ such that $T(N,\lambda) \ll N^2$.*

Lemma 1 is an immediate corollary to the following lemma.

Lemma 2. *For sufficiently large N the arithmetic mean $A(N,M)$ of $T(N,\lambda)$ over all λ in $L(N,M)$ satisfies $A(N,M) \ll N^2$.*

Proof: For any integer k let $P(N,k)$ be the number of ordered quadruples $q = (q_1,q_2,q_3,q_4)$ of *distinct* elements of the set $\{1,2,\ldots,N\}$ satisfying (3), below. We rewrite (3) as (4).

$$(N+q_1)^2 + (N+q_2)^2 - (N+q_3)^2 - (N+q_4)^2 = k \tag{3}$$

$$(q_1-q_3)(2N+q_1+q_3) = (q_4-q_2)(2N+q_2+q_4) + k \tag{4}$$

Note that $P(N,k) = P(N,-k)$ for all integers k.

Assume $k \geq 0$. Denote the right-hand side of (4) by $h+k$. We have the following relations.

$$\sqrt{|h+k|} \leq 2N+q_1+q_3 \leq 4N, \quad 2N+q_1+q_3 \text{ divides } h+k \tag{5}$$

$$\sqrt{|h|} \leq 2N+q_2+q_4 \leq 4N, \quad 2N+q_2+q_4 \text{ divides } h \tag{6}$$

$$-3N^2 \leq h \leq 3N^2 \tag{7}$$

Motivated by (5), (6) and (7) we define, for any integer h, $\tau_1(h)$ to be the number of positive integers s satisfying $\sqrt{|h|} \leq s \leq 4N$, s divides h. It is immediate that

$$P(N,k) \leq \sum_{-3N^2\leq h\leq 3N^2} \tau_1(h)\tau_1(h+|k|) \quad \text{for all integers } k \tag{8}$$

In Section 2, assuming N is sufficiently large, we will prove the following inequality.

$$A(M,N) \leq 2(N^2 - N) + \frac{1}{2M+1} \sum_{0 \leq |k| \leq 4M} P(N,k) \tag{9}$$

To finish the proof of Lemma 2 we will use the following estimates whose proofs will be given in Section 3. These estimates have perhaps already appeared in the literature in another context. For the lack of suitable references we include their proofs.

$$\sum_{-3N^2 \leq h \leq 3N^2} \tau_1^2(h) \ll N^2 \log(N) \tag{10}$$

$$\sum_{1 \leq k \leq 4N} \sum_{-3N^2 \leq h \leq 3N^2} \tau_1(h)\tau_1(h+k) \ll N^2 M \tag{11}$$

Combining (8)–(11) we obtain (12) below, for sufficiently large N.

$$A(N,M) \ll N^2 \Big(1 + \frac{\log(N)}{M}\Big) \ll N^2 \tag{12}$$

This completes the proof of Lemma 2.

3. An inequality for $A(N,M)$. Lemma 3. *For sufficiently large N inequality (9) holds.*

Proof. Let $\wp(N)$ denote the set of all ordered quadruples $q = (q_1, q_2, q_3, q_4)$ of elements of the set $\{1, 2, \ldots, N\}$ satisfying $q_1 \neq q_2, q_3 \neq q_4$. We will use the letter q to denote a general element of $\wp(N)$. We will denote $L(N,M)$ by L and it's cardinality by $|L|$.

From the definition of $T(N,\lambda)$ given in Section 1 it follows that $T(N,\lambda)$ is the number of q satisfying (13) below for a given λ. We rewrite (13) as (14).

$$(N+q_1)^2 + \lambda(q_1) + (N+q_2)^2 + \lambda(q_2) = (N+q_3)^2 + \lambda(q_3) + (N+q_4)^2 + \lambda(q_4) \tag{13}$$

$$(N+q_1)^2 + (N+q_2)^2 - (N+q_3)^2 - (N+q_4)^2 = \lambda(q_4) + \lambda(q_3) - \lambda(q_1) - \lambda(q_2) \tag{14}$$

$$(N+q_1)^2 + (N+q_2)^2 - (N+q_3)^2 - (N+q_4)^2 = k(q) \tag{15}$$

For any q, we denote the left hand side of (14) by $k(q)$ and denote by $m(q)$ the number of λ in L for which (14) is satisfied by the given q. It then follows that

$$\sum_{\lambda \in L} T(N,\lambda) = \sum_{q \in \wp(N)} m(q) \tag{16}$$

Remark 1. If $|k(q)| > 4M$ then $m(q) = 0$.

Since λ takes values in $[-M, M]$ it follows that the right hand side of (14) lies in $[-4M, 4M]$. Hence the remark.

Remark 2. If $|k(q)| \leq 4M$ and $k(q) \neq 0$ then q_1, q_2, q_3, q_4 are all distinct.

Suppose $q_1 = q_3$. If $q_2 \neq q_4$, then the left hand side of (15) is of the order N while the right hand side if of the order M. Since M is $o(N)$ this gives a contradiction for sufficiently large N. Hence $q_2 = q_4$ and therefore $k(q) = 0$ contradicting $k(q) \neq 0$. Thus $q_1 \neq q_3$. In a similar manner we dispose off all possibilities of equality between q_1, q_2, q_3, q_4 till we arrive at the remark. Note that $q_1 = q_2$ or $q_3 = q_4$ are impossible by definition of $\wp(N)$.

Let $\wp_1(N)$ consist of all those q with either $q_1 = q_3$ and $q_2 = q_4$ or $q_1 = q_4$ and $q_2 = q_3$. The cardinality of $\wp_1(N)$ is clearly $2(N^2 - N)$. Further $k(q) = 0$ for q in $\wp_1(N)$. Also one has

Remark 3. If $k(q) = 0$ then either q_1, q_2, q_3, q_4 are distinct or q is in $\wp_1(N)$.

Combining the above remarks we have (17), below,where $\sum^1$ denotes that the summation is only over those q with q_1, q_2, q_3, q_4 distinct.

$$\sum_{q \in \wp(N)} m(q) = \sum_{q \in \wp_1(N)} m(q) + \sum_{0 \leq |k| \leq 4M}^{1} m(q) \tag{17}$$

Remark 4. If q is in $\wp_1(N)$ then $m(q)$ is $|L|$.

Remark 5. If the q_1, q_2, q_3, q_4 are distinct then $m(q)$ is at most $|L|/2M + 1$.

When q_1, q_2, q_3, q_4 are distinct then $m(q)$ is at most the number of mappings from an $N - 1$ element subset of $\{1, 2, \ldots, N\}$ into the set of integers in the closed interval $[-M, M]$. This in our notation is $|L|/2M + 1$. Hence Remark 5.

Combining the Remarks (4)–(6) with (17) and recalling the definition of $P(N, k)$ from Section 1, we obtain the inequality (9).

4. Upper bounds for the τ_1 sums. Here we prove (10) and (11). First a lemma.

LEMMA 4. *We have for all integers $k \geq 0$ the following inequality*

$$\sum_{-3N^2 \leq h \leq 3N^2} \tau_1(h)\tau_1(h+k) \leq 4 \sum_{\substack{1 \leq s \leq 4N \\ 1 \leq t \leq 4N}}^{k} \gcd(s, t) \tag{18}$$

Above $\sum^k$ indicates that the summation is only over those (s, t) with $\gcd(s, t)$ dividing k. Note that when k is 0, $\sum^k$ is the same as $\sum$.

Proof. Recalling the definition of τ_1 and interchanging the summations involved we obtain (19), below, where $\sum^1$ indicates that the summation is only over those h in $[-3N^2, 3N^2]$ satisfying the conditions $h \equiv 0 \pmod{s}$ and $h + k \equiv 0$

(mod t). Clearly, the conditions $h \equiv 0 \pmod{s}$ and $h+k \equiv 0 \pmod{t}$ imply that $\gcd(s,t)$ divides k. Hence the appearance of $\sum^k$ in (19).

$$\sum_{-3N^2 \le h \le 3N^2} \tau_1(h)\tau_1(h+k) \le \sum_{\substack{1\le s\le 4N\\ 1\le t\le 4N}}^{k} \ \sum_{\substack{1\le\sqrt{|h|}\le s\\ 1\le\sqrt{|h+k|}\le t}}^{1} 1 \tag{19}$$

Assume that $s \ge t$. The Chinese Remainder Theorem gives an integer p such that for any h satisfying the conditions $h \equiv 0 \pmod{s}$ and $h+k \equiv 0 \pmod{t}$, h satisfies $h \equiv p \pmod{\operatorname{lcm}(s,t)}$. If, in addition, $1 \le \sqrt{|h|} \le s$ then there are at most $2s^2/\operatorname{lcm}(s,t)+1$ such h. With this we obtain the inequalities (20), below. When $s>t$ we argue with $h+k$ in place of h and t in place of s to obtain the same inequalities. Combining (19) and (20), Lemma 4 follows.

$$\sum_{\substack{1\le\sqrt{|h|}\le s\\ 1\le\sqrt{|h+k|}\le t}}^{1} 1 \le \Big(\frac{2s^2}{\operatorname{lcm}(s,t)}+1\Big) = \Big(\frac{2s}{t}\gcd(s,t)+1\Big) \le 4\gcd(s,t) \tag{20}$$

To obtain (10) and (11) we note the following inequalities.

$$\sum_{\substack{1\le s\le 4N\\ 1\le t\le 4N}} \gcd(s,t) = \sum_{1\le l\le 4N} l \sum_{\substack{1\le s\le 4N\\ 1\le t\le 4N}}^{l} 1 \le \sum_{1\le l\le 4N} l\Big(\frac{4N}{l}\Big)^2 \ll N^2\log(N) \tag{21}$$

where $\sum^l$ denotes that the summation is only over those (s,t) for which $\gcd(s,t)$ is l.

$$\sum_{1\le k\le 4M} \sum_{\substack{1\le s\le 4N\\ 1\le t\le 4N}}^{k} \gcd(s,t) = \sum_{1\le m\le 4N} m \sum_{\substack{1\le s,t\le 4N\\ 1\le k\le 4M}}^{m} 1 \le \sum_{1\le m\le 4N} m\Big(\frac{4M}{m}\Big)\Big(\frac{4N}{m}\Big)^2 \ll N^2 M \tag{22}$$

where $\sum^m$ indicates that the summation is only over those (k,s,t) such that $\gcd(s,t)$ is m and m divides k.

Combining (21) and (22) with Lemma 4 we obtain (10) and (11).

5. Acknowledgements. The basic idea that Lemma 2 implies Lemma 1 is in [1]. We thank Dr. Mohan Nair, Prof. A.O.L. Atkin and Mr. Jishnu Biswas.

References

1. A.O.L. Atkin, *On Psuedo-squares*, Proc. London Math. Soc. (A)(3) **14** (1965), 22–27.
2. H. Halberstam and K.F. Roth, *Sequences, Vol. 1*, Oxford University Press, 1966.

The Institute of Mathematical Sciences
C.I.T. Campus, Taramani
Chennai 600113
India
balu@imsc.ernet.in
suri@imsc.ernet.in

(Received 19 01 1998)