ACTA ARITHMETICA
LXI.2 (1992)

Squares in difference sets

by

Jacek Fabrykowski (Winnipeg, Man.)

1. Introduction. There are many problems in number theory that reduce to searching for squares in specific sequences. For instance, we would like to know whether there are infinitely many squares of type $p-1$, where p ranges over primes. Of particular interest is the general problem whether the difference set

$$\mathcal{A}-\mathcal{B}=\{a-b\,;a\in\mathcal{A},\ b\in\mathcal{B}\}$$

contains squares. Furstenberg [1] and Sárközy [3] studied the case $\mathcal{A}=\mathcal{B}$ and gave an affirmative answer under the amazingly general condition that $\mathcal{A}$ has a positive upper density. Sárközy [3] succeeded in proving a quantitative version for thinner sets. The best result (under the weakest assumptions) so far has been established by Pintz, Steiger and Szemerédi [2] showing that $\mathcal{A}-\mathcal{A}$ contains infinitely many squares if

$$\mathcal{A}(x)=\#\{a\in\mathcal{A}\,;a\le x\}>cx(\log x)^{-(1/12)\log\log\log\log x}\,,$$

where c is an absolute positive constant.

Various methods have been employed. Furstenberg used ergodic theory, Sárközy applied the circle method together with a combinatorial idea and Pintz, Steiger and Szemerédi introduced further combinatorial refinements.

In this work we apply a variant of the dispersion method which has a potential to give squares in considerably thinner sets.

Let $\mathcal{A}=(a_m)$ and $\mathcal{B}=(b_n)$ be finite sequences of complex numbers. In applications $\mathcal{A}$ and $\mathcal{B}$ will be considered as characteristic functions of finite sets. Our aim is to evaluate the sum

$$S(\mathcal{A},\mathcal{B})=\sum\sum_{m-n=l^2}\sum a_mb_nl\,. \tag{1}$$

Let $\nu_d(k)$ be the number of solutions to $x^2\equiv k\ (\operatorname{mod} d)$. Put

$$\chi_c(k)=\sum_{d\mid c}\mu\left(\frac{c}{d}\right)\nu_d(k)\quad\text{ and }\quad s_C(k)=\frac12\sum_{c\le C}\chi_c(k)\,.$$

Theorem 1. *Let $C \ge 2$ and $a_m = 0$ for $m > M$. Then*

$$S(\mathcal{A},\mathcal{B}) = \sum\sum_{m>n} a_m b_n s_C(m-n) + \mathcal{E}_C(\mathcal{A},\mathcal{B})\,, \tag{2}$$

where

$$\mathcal{E}_C(\mathcal{A},\mathcal{B}) \ll (C^{-1/2}M + M^{11/12}\log M)\|\mathcal{A}\|\,\|\mathcal{B}\| \tag{3}$$

and

$$\|\mathcal{A}\| = \Big(\sum |a_m|^2\Big)^{1/2}, \qquad \|\mathcal{B}\| = \Big(\sum |b_n|^2\Big)^{1/2}.$$

Remarks. Notice that $\chi_c(k)$ is multiplicative in c. If $(c, 2k) = 1$ we have

$$\chi_c(k) = \left(\frac{k}{c}\right)\mu^2(c)\,. \tag{4}$$

For other c the formula for $\chi_c(k)$ is somewhat complicated but still expressed in terms of the quadratic character.

The error term $\mathcal{E}_C(\mathcal{A},\mathcal{B})$ can be improved a bit by employing the Fourier technique. Regarding the parameter C it yields the best estimate for the error term $\mathcal{E}_C(\mathcal{A},\mathcal{B})$ with $C = M^{1/6}$, however such a choice may not be best for handling the main term. Clearly, for that matter we may want C to be small depending on our knowledge of the distribution of $\mathcal{A}$ and $\mathcal{B}$ in arithmetic progressions. For example, if we deal with primes $\le M$ then we can allow $C \ll (\log M)^A$ in view of the Prime Number Theorem of Siegel and Walfisz.

2. Dispersion method. We set $s(k) = l$ if $k = l^2$ and $s(k) = 0$ otherwise, so

$$S(\mathcal{A},\mathcal{B}) = \sum\sum_{m>n} a_m b_n s(m-n)\,.$$

Therefore Theorem 1 reveals that the character sum $s_C(k)$ approximates $s(k)$ very well in the sense that the bilinear form

$$S_C(\mathcal{A},\mathcal{B}) = \sum\sum_{m>n} a_m b_n s_C(m-n)$$

is close to $S(\mathcal{A},\mathcal{B})$. To estimate the difference $\mathcal{E}_C(\mathcal{A},\mathcal{B}) = S(\mathcal{A},\mathcal{B}) - S_C(\mathcal{A},\mathcal{B})$ we shall apply the dispersion method.

Let us introduce

$$S(n) = \sum_{m>n} a_m s(m-n)\,, \qquad S_C(n) = \sum_{m>n} a_m s_C(m-n)\,,$$

and

$$S_C = \sum\sum_{m>n} a_m b_n s_C(m-n)\,.$$

By Cauchy's inequality we obtain

$$\mathcal{E}_C(\mathcal{A},\mathcal{B}) = \sum_n b_n(S(n) - S_C(n)) \ll D^{1/2}\|\mathcal{B}\|\,, \tag{5}$$

where

$$D = \sum_n |S(n) - S_C(n)|^2\,.$$

Squaring out and changing the order of summation we write

$$D = \langle S, S\rangle - 2\,\mathrm{Re}\langle S, S_C\rangle + \langle S_C, S_C\rangle\,, \tag{6}$$

where

$$\langle S,S\rangle = \sum_n |S(n)|^2,\quad \langle S,S_C\rangle = \sum_n S(n)\overline{S_C(n)},\quad \langle S_C,S_C\rangle = \sum_n |S_C(n)|^2,$$

with the aim of evaluating each sum separately.

3. Evaluation of $\langle S_C, S_C\rangle$. We have

$$\begin{aligned}\langle S_C,S_C\rangle &= \sum_n \sum_{m_1>n}\sum_{m_2>n} a_{m_1}\overline{a}_{m_2} s_C(m_1-n)s_C(m_2-n)\\ &= \frac{1}{4}\sum\sum_{c_1,c_2\le C}\sum_{m_1}\sum_{m_2} a_{m_1}\overline{a}_{m_2}\mathcal{J}_{c_1c_2}(m_1,m_2)\,,\end{aligned}$$

where

$$\mathcal{J}_{c_1c_2}(m_1,m_2) = \sum_{n<\min(m_1,m_2)} \chi_{c_1}(m_1-n)\chi_{c_2}(m_2-n)\,.$$

Since $\chi_c(k)$ is periodic in k of period c we split the summation over n into progressions to modulus c_1c_2 and get

$$\begin{aligned}\mathcal{J}_{c_1c_2}(m_1,m_2) &= \sum_{z\,(\mathrm{mod}\,c_1c_2)} \chi_{c_1}(m_1-z)\chi_{c_2}(m_2-z)\Big(\frac{\min(m_1,m_2)}{c_1c_2} + O(1)\Big)\\ &= \frac{\min(c_1,c_2)}{c_1c_2}\mathrm{j}_{c_1c_2}(m_1-m_2) + O(c_1c_2)\,,\end{aligned}$$

where

$$\mathrm{j}_{c_1c_2}(k) = \sum_{z\,(\mathrm{mod}\,c_1c_2)} \chi_{c_1}(z)\chi_{c_2}(z-k)\,, \tag{7}$$

which resembles the Jacobi sum. Here the error term comes from the trivial estimate

$$\sum_{z\,(\mathrm{mod}\,c_1c_2)} |\chi_{c_1}(z)\chi_{c_2}(z-k)| \ll c_1c_2\,. \tag{8}$$

For exact evaluation of $\mathrm{j}_{c_1c_2}(k)$ we appeal to the formula for the Ramanujan sum

$$R_c(k) = \sum_{x \,(\mathrm{mod}\, c)}^{*} e\Big(\frac{kx}{c}\Big) = \sum_{\substack{d\mid c\\ d\mid k}} d\mu\Big(\frac{c}{d}\Big) \tag{9}$$

giving

$$\chi_c(k) = \frac{1}{c} \sum_{x \,(\mathrm{mod}\, c)} \sum_{y \,(\mathrm{mod}\, c)}^{*} e\Big(\frac{y(x^2-k)}{c}\Big). \tag{10}$$

Hence

$$\mathrm{j}_{c_1c_2}(k) = \frac{1}{c_1c_2} \sum\sum_{\substack{x_1 \,(\mathrm{mod}\, c_1)\\ x_2 \,(\mathrm{mod}\, c_2)}} \sum^{*}\sum^{*}_{\substack{y_1 \,(\mathrm{mod}\, c_1)\\ y_2 \,(\mathrm{mod}\, c_2)}} \sum_{z \,(\mathrm{mod}\, c_1c_2)} e\Big(\frac{y_1(x_1^2-z)}{c_1} - \frac{y_2(x_2^2-z+k)}{c_2}\Big).$$

Here the innermost sum vanishes unless $c_1 = c_2 = c$ say, and $y_1 \equiv y_2 \ (\mathrm{mod}\, c)$, in which case we get

$$\mathrm{j}_{cc}(k) = \sum_{y \,(\mathrm{mod}\, c)}^{*} \sum\sum_{x_1,x_2 (\mathrm{mod}\, c)} e\Big(\frac{y(x_1^2-x_2^2-k)}{c}\Big) = |G(c)|^2 R_c(k)\,,$$

where $G(c)$ is the Gauss sum

$$G(c) = \sum_{x \,(\mathrm{mod}\, c)} e\Big(\frac{x^2}{c}\Big).$$

For subsequent use we recall the well-known formula

$$|G(c)|^2 = \begin{cases} c & \text{if } 2\nmid c,\\ 0 & \text{if } 2\,\|\, c,\\ 2c & \text{if } 4\mid c. \end{cases} \tag{11}$$

Collecting the above evaluations we conclude that

$$\begin{aligned} \langle S_C, S_C\rangle &= \frac{1}{4} \sum_{c\le C} c^{-2}|G(c)|^2 \sum_{m_1}\sum_{m_2} a_{m_1}\overline{a}_{m_2} \min(m_1,m_2) R_c(m_1-m_2)\\ &\quad + O\Big(C^4\Big(\sum_m |a_m|\Big)^2\Big). \end{aligned} \tag{12}$$

4. Evaluation of $\langle S, S_C\rangle$. We have

$$\begin{aligned}\langle S, S_C\rangle &= \sum_{n}\sum_{m_1>n}\sum_{m_2>n} a_{m_1}\overline{a}_{m_2} s(m_1-n)s_C(m_2-n)\\ &= \frac{1}{2}\sum_{c\le C}\sum_{m_1}\sum_{m_2} a_{m_1}\overline{a}_{m_2}\mathcal{J}_c(m_1,m_2)\,,\end{aligned}$$

where

$$\begin{aligned}\mathcal{J}_c(m_1,m_2) &= \sum_{n<\min(m_1,m_2)} s(m_1-n)\chi_c(m_2-n)\\ &= \sum_{0<m_1-l^2<\min(m_1,m_2)} \chi_c(l^2+m_2-m_1)l\\ &= \sum_{z\,(\mathrm{mod}\,c)} \chi_c(z^2+m_2-m_1)\Big(\sum_{\substack{l\equiv z\,(\mathrm{mod}\,c)\\ 0<m_1-l^2<\min(m_1,m_2)}} l\Big)\\ &= \frac{\min(m_1,m_2)}{2c}\,\mathrm{j}_c(m_2-m_1)+O(cm_1^{1/2})\,,\end{aligned}$$

where

$$\mathrm{j}_c(k)=\sum_{z\,(\mathrm{mod}\,c)}\chi_c(z^2+k) \tag{13}$$

and the error term comes from the trivial estimate

$$\sum_{z\,(\mathrm{mod}\,c)} |\chi_c(z^2+k)| \ll c\,. \tag{14}$$

By (10) and (13) we infer that

$$\mathrm{j}_c(k)=\frac{1}{c}\sum_{x\,(\mathrm{mod}\,c)}\sideset{}{^*}\sum_{y\,(\mathrm{mod}\,c)}\sum_{z\,(\mathrm{mod}\,c)} e\Big(\frac{y(x^2-z^2-k)}{c}\Big)=\frac{|G(c)|^2}{c}R_c(k)\,.$$

Collecting the above evaluations we conclude that

$$\begin{aligned}\langle S, S_C\rangle &= \frac{1}{4}\sum_{c\le C} c^{-2}|G(c)|^2\sum_{m_1}\sum_{m_2} a_{m_1}\overline{a}_{m_2}\min(m_1,m_2)R_c(m_2-m_1)\\ &\quad + O\Big(C^2\Big(\sum_m m^{1/2}|a_m|\Big)\Big(\sum_m |a_m|\Big)\Big)\,.\end{aligned} \tag{15}$$

5. Evaluation of $\langle S,S\rangle$. We have

$$\begin{aligned}\langle S,S\rangle &= 2\,\mathrm{Re}\sum\sum_{n<m_2<m_1}\sum a_{m_1}\overline{a}_{m_2}s(m_1-n)s(m_2-n)+\sum_{l^2<m}\sum l^2|a_m|^2\\ &= 2\,\mathrm{Re}\sum_{m_2<m_1}\sum a_{m_1}\overline{a}_{m_2}\mathcal{J}(m_1,m_2)+O\Big(\sum_m m^{3/2}|a_m|^2\Big),\end{aligned}$$

where

$$\mathcal{J}(m_1,m_2)=\sum_{n<m_2}\sum s(m_1-n)s(m_2-n)\,.$$

To evaluate $\mathcal{J}(m_1,m_2)$ we put $n=m_1-l_1^2=m_2-l_2^2$ and then $u=l_1-l_2$, $v=l_1+l_2$. This is a one-to-one correspondence subject to the following conditions:

$$U_1<u<U_2\,,\qquad uv=k\,,\qquad u\equiv v \pmod 2\,,$$

where $U_1=\sqrt{m_1}-\sqrt{m_2}$, $U_2=\sqrt{m_1-m_2}$ and $k=m_1-m_2$.

Hence we obtain

$$\begin{aligned}\mathcal{J}(m_1,m_2)&=\frac14\sum_u\sum_v(v^2-u^2)=\frac14\sum_{\substack{U_1<u<U_2\\ k\equiv u^2 \,(\mathrm{mod}\, 2u)}}(k^2u^{-2}-u^2)\\ &=\frac14\sum_{U_1<u<U_2}(k^2u^{-2}-u^2)\frac{1}{2u}\sum_{y\,(\mathrm{mod}\,2u)}e\Big(\frac{y(k-u^2)}{2u}\Big)\\ &=\sum_{\substack{2U_1<cr<2U_2\\ 2|cr}}(cr)^{-1}\Big[\Big(\frac{k}{cr}\Big)^2-\Big(\frac{cr}{4}\Big)\Big]\sum_{x\,(\mathrm{mod}\,c)}^{*}e\Big(\frac{xk}{c}+\frac{xcr^2}{4}\Big)\\ &=H(m_1,m_2)+I(m_1,m_2)\,,\end{aligned}$$

say, where $H(m_1,m_2)$ denotes the partial sum restricted by $c\le C$ and $I(m_1,m_2)$ denotes the partial sum restricted by $c>C$.

First we evaluate $H(m_1,m_2)$. Given $c\le C$ we sum over r getting

$$\begin{aligned}&\sum_{\substack{R_1<r<R_2\\ 2|(2,c)r}}r^{-1}\Big[\Big(\frac{k}{cr}\Big)^2-\Big(\frac{cr}{4}\Big)^2\Big]e\Big(\frac{xcr^2}{4}\Big)\\ &\qquad=\sum_{\substack{\varrho\,(\mathrm{mod}\,2)\\ 2|(2,c)\varrho}}e\Big(\frac{xc\varrho^2}{4}\Big)\sum_{\substack{R_1<r<R_2\\ r\equiv\varrho\,(\mathrm{mod}\,2)}}r^{-1}\Big[\Big(\frac{k}{cr}\Big)^2-\Big(\frac{cr}{4}\Big)^2\Big],\end{aligned}$$

where $R_1=2U_1c^{-1}$ and $R_2=2U_2c^{-1}$. The innermost sum is approximated by

$$\frac{1}{2}\int\limits_{R_1}^{R_2}\left[\left(\frac{k}{cr}\right)^2-\left(\frac{cr}{4}\right)^2\right]\frac{dr}{r}+O\left(\frac{m_1}{R_1}\right)=\frac{m_2}{4}+O\left(\frac{cm_1}{\sqrt{m_1}-\sqrt{m_2}}\right)$$

and the outer sum is clearly equal to $|G(c)|^2c^{-1}$ (see (11)). This gives

$$H(m_1,m_2)=\frac{1}{4}\sum_{c\le C}c^{-2}|G(c)|^2m_2R_c(m_1-m_2)+O\left(\frac{Cm_1}{\sqrt{m_1}-\sqrt{m_2}}\right).$$

Now we proceed to estimate $I(m_1,\ m_2)$ by an appeal to the large sieve inequality

$$\sum_{q\le Q}\ \sideset{}{^*}\sum_{a(\operatorname{mod} q)}\Big|\sum_{m\le M}\lambda_m e\Big(\frac{a}{q}m\Big)\Big|^2\le(Q^2+M)\sum_{m\le M}|\lambda_m|^2\,. \tag{16}$$

We assume that the sequence $\mathcal{A}=(a_m)$ is supported in the interval $1\le m\le M$ and deduce by partial summation that

$$\begin{aligned}\sum_{m_2<m_1}\sum & a_{m_1}\overline{a}_{m_2}I(m_1,m_2)\\ &\ll C^{-1}M(\log M)^2\sum_{c\le 2\sqrt{M}}\ \sideset{}{^*}\sum_{x\,(\operatorname{mod} c)}\Big|\sum_{m\le M}a'_m e\Big(\frac{x}{c}m\Big)\Big|\Big|\sum_{m\le M}a''_m e\Big(\frac{x}{c}m\Big)\Big|\end{aligned}$$

with some sequences $\mathcal{A}'=(a'_m)$ and $\mathcal{A}''=(a''_m)$ with $|a'_m|\le|a_m|$ and $|a''_m|\le|a_m|$. Hence by (16) the above sum is

$$\ll C^{-1}M^2(\log M)^2\sum_{m\le M}|a_m|^2\,.$$

Collecting the above results we conclude that

$$\begin{aligned}(17)\quad \langle S,S\rangle &\\ =\ &\frac{1}{4}\sum_{c\le C}c^{-2}|G(c)|^2\sum_{m_1}\sum_{m_2}a_{m_1}\overline{a}_{m_2}\min(m_1,m_2)R_c(m_1-m_2)\\ &+O\Big((CM^{3/2}+C^{-1}M^2)(\log M)^2\Big(\sum_m|a_m|^2\Big)\Big)\,.\end{aligned}$$

6. Proof of Theorem 1. Conclusion. Inserting (12), (15) and (17) to (6) we find that the main terms cancel out and we are left with the error terms giving

$$D\ll(C^4M+C^2M^{3/2}+C^{-1}M^2)(\log M)^2\Big(\sum_m|a_m|^2\Big)\,. \tag{18}$$

Finally, by (5) we get (2) with

$$\mathcal{E}_C(\mathcal{A},\mathcal{B})\ll(C^2M^{-1/2}+CM^{3/4}+C^{-1/2}M)(\log M)\|\mathcal{A}\|\,\|\mathcal{B}\|\,.$$

We shall improve this result slightly by estimating the difference

$$S_C(\mathcal{A},\mathcal{B}) - S_{C_0}(\mathcal{A},\mathcal{B}) = \frac{1}{2}\sum_{C_0<c\le C}\sum_{m>n}\sum a_m b_n \chi_c(m-n)\,.$$

Using the results of Section 3 and the large sieve inequality we obtain

$$\begin{aligned}
&|S_C(\mathcal{A},\mathcal{B}) - S_{C_0}(\mathcal{A},\mathcal{B})|^2 \\
&\quad \le \|\mathcal{B}\|^2 \sum_n \Big|\sum_{C_0<c\le C}\sum_{m>n} a_m \chi_c(m-n)\Big|^2 \\
&\quad = \|\mathcal{B}\|^2 \sum_{C_0<c_1,c_2\le C}\sum_{m_1}\sum_{m_2} a_{m_1}\overline{a}_{m_2}\mathcal{J}_{c_1c_2}(m_1,m_2) \\
&\quad = \|\mathcal{B}\|^2 \sum_{C_0<c\le C} c^{-2}|G(c)|^2 \sum_{m_1}\sum_{m_2} a_{m_1}\overline{a}_{m_2}\min(m_1,m_2)R_c(m_1-m_2) \\
&\qquad + O(C^4M\|\mathcal{A}\|^2\|\mathcal{B}\|^2) \\
&\quad \ll (C_0^{-1}M^2 + C^4M)\|\mathcal{A}\|^2\|\mathcal{B}\|^2\,.
\end{aligned}$$

This gives

$$\begin{aligned}
S(\mathcal{A},\mathcal{B}) &= S_{C_0}(\mathcal{A},\mathcal{B}) \\
&\quad + O([(C^2M^{1/2} + CM^{3/4} + C^{-1/2}M)\log M + C_0^{-1/2}M]\|\mathcal{A}\|\|\mathcal{B}\|)\,.
\end{aligned}$$

We take $C = M^{1/6}$ and get (2) with (3).

7. Further assumptions and results. Our goal is to give a more accessible expression for the main term $S_C(\mathcal{A},\mathcal{B})$ in Theorem 1. To this end we impose local conditions on the distribution of squares in the difference set. Suppose the sequences $\mathcal{A},\mathcal{B}$ satisfy the asymptotic law

$$\sum_{m>n}\sum a_m b_n \nu_d(m-n) = \omega(d)\sum_{m>n} a_m b_n + r_d(\mathcal{A},\mathcal{B})\,,$$

where $r_d(\mathcal{A},\mathcal{B})$ is considered as an error term and $\omega(d)$ is a multiplicative function such that

$$Z(s) = \zeta^{-1}(s)\sum_{d=1}^{\infty}\omega(d)d^{-s} \tag{19}$$

is holomorphic and bounded in $\operatorname{Re} s \ge -1/2$. We obtain

$$S_C(\mathcal{A},\mathcal{B}) = \frac{1}{2}\sum_{c\le C}\Big(\sum_{d\mid c}\omega(d)\mu\Big(\frac{c}{d}\Big)\Big)\sum_{m>n}\sum a_m b_n + \mathcal{F}_C(\mathcal{A},\mathcal{B})\,,$$

where

$$|\mathcal{F}_C(\mathcal{A},\mathcal{B})| \le \sum_{d\le C} Cd^{-1}|r_d(\mathcal{A},\mathcal{B})|\,. \tag{20}$$

Furthermore, by contour integration we find that

$$\begin{aligned}\sum_{c\le C}\Big(\sum_{d\mid c}\omega(d)\mu\Big(\frac{c}{d}\Big)\Big)\\ &= \frac{1}{2\pi i}\int_{1/2-iT}^{1/2+iT} Z(s)C^s\frac{ds}{s} + O(T^{-1}C^{1/2}\log C)\\ &= Z(0) + \frac{1}{2\pi i}\int_{-1/2-iT}^{-1/2+iT} Z(s)C^s\frac{ds}{s} + O(T^{-1}C^{1/2}\log C)\\ &= Z(0) + O(C^{-1/2}\log T + T^{-1}C^{1/2}\log C)\\ &= Z(0) + O(C^{-1/2}\log C)\end{aligned}$$

by taking $T = C$. Hence we conclude the following

THEOREM 2. *Under the above conditions we have*

$$\begin{aligned}S(\mathcal{A},\mathcal{B}) = \frac{1}{2}Z(0)\sum_{m>n}\sum a_m b_n + \mathcal{F}_C(\mathcal{A},\mathcal{B})\\ + O(MC^{-1/2}\log C + M^{11/12}\log M)\|\mathcal{A}\|\|\mathcal{B}\|\,.\end{aligned}$$

8. An application. To illustrate the asymptotic formula of Theorem 2 we consider the sequences $\mathcal{A} = \mathcal{B} = (\Lambda(n))$, the von Mangoldt function. By the Generalized Riemann Hypothesis we get

$$\sum_{n<m\le M}\sum \Lambda(m)\Lambda(n)\nu_d(m-n) = \omega(d)\sum_{n<m\le M}\sum \Lambda(m)\Lambda(n) + r_d(\mathcal{A},\mathcal{B})\,,$$

where

$$\omega(d) = \frac{1}{\varphi^2(d)}\sum^*\sum^*_{\alpha,\beta(\operatorname{mod} d)}\nu_d(\alpha-\beta) = 1$$

and

$$r_d(\mathcal{A},\mathcal{B}) \ll (dM^{3/2} + d^2M)(\log M)^2\,.$$

Hence

$$\mathcal{F}_C(\mathcal{A},\mathcal{B}) \ll (C^2M^{3/2} + C^3M)(\log M)^2\,.$$

COROLLARY. *We have*

$$\sum_{n<m\le M}\sum \Lambda(m)\Lambda(n)s(m-n) = \tfrac{1}{4}M^2 + O(M^{23/12}\log M)\,.$$

Remark. Assuming no Riemann hypothesis one gets the above asymptotics with the error term $O(M^2(\log M)^{-A})$ for any $A > 0$, and the implied constant depending on A.

References

[1] H. Furstenberg, *Ergodic behavior of diagonal measures and a theorem of Szemerédi on arithmetic progressions*, J. Analyse Math. 31 (1977), 204–256.
[2] J. Pintz, W. L. Steiger and E. Szemerédi, *On sets of natural numbers whose difference set contains no squares*, J. London Math. Soc. (2) 37 (1988), 219–231.
[3] A. Sárközy, *On difference sets of sequences of integers. I*, Acta Math. Acad. Sci. Hungar. 31 (1978), 125–149.

DEPARTMENT OF MATHEMATICS AND ASTRONOMY
UNIVERSITY OF MANITOBA
WINNIPEG, MANITOBA
CANADA R3T 2N2

Received on 3.7.1991 (2156)