LMS J. Comput. Math. 15 (2012) 59–70 © 2012 Author
doi:10.1112/S1461157012000058

Products of three pairwise coprime integers in short intervals

Asim Islam

Abstract

The existence of products of three pairwise coprime integers is investigated in short intervals of the form $(x, x + x^{\frac{1}{2}}]$. A general theorem is proved which shows that such integer products exist provided there is a bound on the product of any two of them. A particular case of relevance to elliptic curve cryptography, where all three integers are of order $x^{\frac{1}{3}}$, is presented as a corollary to this result.

1. *Introduction*

We investigate the existence of a product of three pairwise coprime integers in the interval $(x, x + y]$ where $y = x^{\frac{1}{2}}$. The approach to the problem is to suppose that one of the integers is a prime p where $p \sim P$ and that the remaining two integers m and n are coprime, where we let $n \sim N$. Here N and P satisfy $NP \leqslant x^{\frac{3}{4}}$, where N is a positive integer such that $2N$ is less than P and $a \sim A$ indicates that $A \leqslant a \leqslant 2A$. We then count products of integers mnp, with $p \nmid m$, in the interval $(x, x + x^{\frac{1}{2}}]$ and show that for sufficiently large x an asymptotic formula exists for the total. This is achieved by considering the case where there are no divisibility conditions between p and m, and the case of $p \mid m$, where $n < p$. The former case generates a main term, and all the error terms arising from the sums in the remaining situations are shown to be smaller than this main term. As a corollary to this result, we prove the existence of three such integers where the order of each integer is $x^{\frac{1}{3}}$ and show that there are pairwise coprime integers of this form in the interval for sufficiently large x.

Problems relating to the existence of such pairwise coprime integers have arisen in the study of elliptic curve cryptography. In a discussion at Royal Holloway with Professor Glyn Harman, Professor Steven Galbraith pointed out that no formal proof was known for the existence of three pairwise coprime integers in short intervals, despite this forming the basis of some protocols. In particular, it had been noted that Bentahar [**3**] required the existence of three coprime integers of roughly equal size $x^{\frac{1}{3}}$ in relation to a certain elliptic curve cryptographic protocol. The arguments used in his paper to show their existence were heuristic, involving probabilistic reasoning but without formal proof. Similarly, Muzereau *et al.* [**9**] considered products of three primes in short intervals. Both [**3**] and [**9**] assumed the existence of these numbers in applications to public key cryptography; the motivation for the present work was to produce a formal proof of the result assumed by these papers. In fact, a more general result is established in the form of Theorem 1, and the particular case of equal-order terms is given as a corollary.

Let $I = (x, x + y]$ be an interval with $y = x^{\frac{1}{2}}$. Our aim is to count products $mnp \in I$ such that $(m, n) = 1$. Since $2N < P$, we suppose $n < p$. Hence consider the sum

$$\sum_{\substack{mnp \in I \\ (m,n)=1, p \nmid m}} 1 = \sum_{\substack{mnp \in I \\ (m,n)=1}} 1 - \sum_{\substack{mnp \in I \\ (m,n)=1, p \mid m}} 1. \tag{1}$$

Received 15 August 2010; revised 11 November 2011.
2000 Mathematics Subject Classification 11N25 (primary).

We begin by looking at the first sum on the right-hand side of (1), where no divisibility conditions are imposed on p and m. This sum can be re-expressed as a double sum involving the Möbius function in the following way:

$$\begin{aligned}\sum_{\substack{mnp\in I\\(m,n)=1}} 1 &= \sum_{mnp\in I}\sum_{r|(m,n)} \mu(r)\\ &= \sum_{r}\mu(r)\sum_{\substack{mnp\in I\\ r|m,r|n}} 1\\ &= \sum_{r}\mu(r)\sum_{m'n'pr^2\in I} 1. \end{aligned} \tag{2}$$

Therefore, we need to count integers of the form $m'n'pr^2 \in I$ where, now, in the inner sum of (2), r is a common divisor of m and n, and we have $m = m'r, n = n'r$.

It will be shown that when r is a large common factor, greater than a certain power of $\log x$, the bound can quickly be obtained by elementary methods. The case of r being a smaller common factor is more involved and, to achieve the result, Fourier methods will be required to obtain a suitable non-trivial bound on a type I sum.

The main term (see (11)) will be obtained for small r and is of order $\gg y/\log x$, while the error term will be

$$O\left(\frac{y}{(\log x)^2} + x^{\frac{1}{3}+3\epsilon} + \frac{y}{x^{\eta}} + x^{\frac{2}{5}} + yx^{\epsilon-\frac{1}{8}}\right). \tag{3}$$

We prove the following theorem and corollary.

THEOREM 1. *Given $\epsilon > 0$, there exists $x_0(\epsilon) > 0$ such that for all $x \geqslant x_0(\epsilon)$ and all positive integers N and P with $x^{\epsilon} < 2N < P < x^{\frac{2}{5}-\epsilon}$ and*

$$NP \leqslant x^{\frac{3}{4}},$$

there exist numbers $mnp \in (x, x + x^{\frac{1}{2}}]$ with $n \sim N$, $p \sim P$ and m, n, p pairwise coprime.

COROLLARY. *For all sufficiently large x there exist integers $mnp \in (x, x + x^{\frac{1}{2}}]$, with $n < p$, where*

$$\frac{x^{\frac{1}{3}}}{2} \leqslant m, n, p \leqslant 2x^{\frac{1}{3}}$$

and m, n, p are pairwise coprime.

2. *Case of large common factors $r > (\log x)^A$*

Consider that part of the inner sum in (2) for which r is larger than a power of $\log x$. Essentially, we count the number of integers of the form $m'n'pr^2 \in I$ or, equivalently, integers of the form $m'n'p \in (x/r^2, (x + y)/r^2]$. Since the number of such products $m'n'p$ is bounded by the three-fold divisor function $\tau_3(k) = \sum_{a_1a_2a_3=k} 1$, we have

$$\sum_{m'n'pr^2\in I} 1 \leqslant \sum_{x/r^2\leqslant k\leqslant x/r^2+y/r^2} \tau_3(k).$$

We appeal to the following lemma by Shiu [**10**].

LEMMA 1. *Given any $\epsilon > 0$ and $Z > W^{\epsilon}$,*

$$\sum_{W\leqslant k\leqslant W+Z} \tau_3(k) \ll Z(\log W)^2$$

where $\tau_3(k)$ is the three-fold divisor function.

https://doi.org/10.1112/S1461157012000058 Published online by Cambridge University Press

Since $n<p$ and r divides both m and n, if $n>x^{\frac{1}{3}}$ then $p>x^{\frac{1}{3}}$, and then $mnp\in(x,x+x^{\frac{1}{2}}]$ only if $m<2x^{\frac{1}{3}}$. Hence we have the restriction $r<2x^{\frac{1}{3}}$ on the size of r (which is smaller than the bound $r<x^{\frac{2}{5}-\epsilon}$ implied by the hypotheses). However, by this lemma with $W=x/r^2$ and $Z=y/r^2$, the condition $Z>W^{\epsilon}$ is satisfied only for $r<x^{\frac{1}{4}-\epsilon}$, and in this range we quickly obtain the bound

$$\sum_{m'n'pr^2\in I}1\ll\frac{y}{r^2}\left(\log\frac{x}{r^2}\right)^2\ll\frac{y}{r^2}(\log x)^2.$$

Letting $L=(\log x)^A$, we obtain the result that for this part of the required sum (2) we have the bound

$$\sum_{r>L}\mu(r)\sum_{m'n'pr^2\in I}1\ll\sum_{r>L}\frac{y}{r^2}(\log x)^2=y(\log x)^2\sum_{r>L}\frac{1}{r^2}.$$

By comparison with an integral, the final sum provides the bound

$$\sum_{r>L}\mu(r)\sum_{m'n'pr^2\in I}1\ll\frac{y(\log x)^2}{L}.$$

Thus, for large x and a suitable choice of A in $L=(\log x)^A$, this bound will be smaller than the main term, as discussed in Section 1 (see (3) for the explicit error term which is to be obtained).

Next, consider the range $x^{\frac{1}{4}-\epsilon}<r<2x^{\frac{1}{3}}$. Using $\tau_3(n)\ll n^{\epsilon}$, we obtain

$$\begin{aligned}\sum_{m'n'pr^2\in I}1=\sum_{m'n'p\in(x/r^2,(x+y)/r^2]}1\leqslant\sum_{n\in(x/r^2,(x+y)/r^2]}\tau_3(n)\leqslant\sum_{n\in(x/r^2,(x+y)/r^2]}n^{\epsilon}\\ \ll x^{\epsilon}(1+y/r^2)\leqslant 2x^{3\epsilon},\end{aligned}$$

since in the range of r under consideration we have $y/r^2<x^{2\epsilon}$. Therefore the sum (1) for this range gives the bound

$$\sum_{x^{\frac{1}{4}-\epsilon}<r<2x^{\frac{1}{3}}}\mu(r)\sum_{m'n'pr^2\in I}1\ll\sum_{x^{\frac{1}{4}-\epsilon}<r<2x^{\frac{1}{3}}}\sum_{m'n'pr^2\in I}1\ll x^{\frac{1}{3}+3\epsilon},$$

which will be smaller than the main term (see Section 1 and, in particular, (3)).

Hence, for the complete range of possible values of $r>L$, we obtain

$$\sum_{r>L}\mu(r)\sum_{m'n'pr^2\in I}1\ll\frac{y(\log x)^2}{L}+x^{\frac{1}{3}+3\epsilon}. \tag{4}$$

3. *Case where p divides m*

Before proceeding to deal with that part of sum (2) for smaller common factors r (see the next section), we consider the second sum on the right-hand side of (1): the case where $p\mid m$.

In order to count the number of times p divides m, first observe that if $P<x^{\frac{1}{8}}$, we can give a completely elementary proof to the whole theorem quickly, since we have $NP^2\leqslant x^{\frac{3}{8}}<x^{\frac{1}{2}}$ (that is, we can always count the number of integers in intervals of the form $(x/np^2,(x+y)/np^2]$ accurately). Henceforth we can assume that $P>x^{\frac{1}{8}}$. Letting $m=m'p$, so that $mnp=m'np^2$, the total number of solutions with $p\mid m$ is

$$\begin{aligned}\leqslant\sum_{p\sim P}\sum_{n\sim N}\sum_{m'np^2\in I}1\ll\sum_{p\sim P}\left(1+\frac{y}{p^2}\right)x^{\epsilon}=x^{\epsilon}\sum_{p\sim P}1+yx^{\epsilon}\sum_{p\sim P}\frac{1}{p^2}\\ \ll x^{\frac{2}{5}}+yx^{\epsilon-\frac{1}{8}},\end{aligned}$$

https://doi.org/10.1112/S1461157012000058 Published online by Cambridge University Press

where we have used the bounds $x^{\frac{1}{8}} < P < x^{\frac{2}{5}-\epsilon}$ in the first sum on the right-hand side of the equality above. For the second sum on the right, observe that there are no more than P terms, each of which is less than $1/P^2$, so that the sum is bounded by $1/P$ and hence by $x^{-\frac{1}{8}}$. The bound obtained here is of smaller order than the main term (see Section 1 and, in particular, (3)).

4. *Case of small common factors $r < (\log x)^A$*

We now consider the inner sum (2) in the case where r is smaller than a power of $\log x$. Suppose $r < L$; then since $m'n'pr^2 \in (x, x+y]$, we have

$$x \leqslant m'n'pr^2 \leqslant x+y \quad \text{so that} \quad \frac{x}{pr^2} \leqslant m'n' \leqslant \frac{x+y}{pr^2}.$$

Letting $J = (x/pr^2, (x+y)/pr^2]$, we may write

$$\sum_{m'n'pr^2 \in I} 1 = \sum_{\substack{m'n' \in J \\ n = n'r \sim N,\ p \sim P}} 1 = \sum_{\substack{m'n' \in J \\ n' \sim N/r,\ p \sim P}} 1.$$

Next, define $\chi(m)$ to be the number of integers in J divisible by m (using square brackets to denote the integer part), as follows:

$$\chi(m) = \sum_{\substack{k \in J \\ m \mid k}} 1 = \left[\frac{x+y}{pmr^2}\right] - \left[\frac{x}{pmr^2}\right].$$

Letting $\psi = \{x\} - 1/2$, where the brace denotes the fractional part, we may write $\chi(m)$ as

$$\chi(m) = \frac{y}{pmr^2} + \psi\left(\frac{x}{pmr^2}\right) - \psi\left(\frac{x+y}{pmr^2}\right).$$

This can be used to re-express the sum under consideration as a main term with fractional parts:

$$\begin{aligned}\sum_{\substack{m'n' \in J \\ n' \sim N/r, p \sim P}} 1 &= \sum_{\substack{n' \sim N/r \\ p \sim P}} \chi(n') \\ &= \sum_{\substack{n' \sim N/r \\ p \sim P}} \frac{y}{n'pr^2} + \sum_{\substack{n' \sim N/r \\ p \sim P}} \left(\psi\left(\frac{x}{n'pr^2}\right) - \psi\left(\frac{x+y}{n'pr^2}\right)\right) \\ &= S_1 + S_2,\end{aligned}$$

say. The sum S_2 will be expressed as an exponential sum with an error term. We aim to show that sufficient savings may be achieved in the subsequent exponential sum such that the error terms will be smaller than the term S_1 and the main term (refer to (11) and Section 1, formula (3)) which it will generate.

Before proceeding, we consider the sum S_1 in more detail by first writing

$$S_1 = \sum_{\substack{n' \sim N/r \\ p \sim P}} \frac{y}{n'pr^2} = \frac{y}{r^2} \sum_{n' \sim N/r} \frac{1}{n'} \sum_{p \sim P} \frac{1}{p}.$$

The first sum on the right, being over consecutive integers, can be approximated by using the standard asymptotic formula

$$\sum_{n \leqslant A} \frac{1}{n} = \log A + C + O\left(\frac{1}{A}\right),$$

https://doi.org/10.1112/S1461157012000058 Published online by Cambridge University Press

from which we obtain

$$\sum_{n'\sim N/r}\frac{1}{n'}=\log 2+O\left(\frac{r}{N}\right).$$

To deal with the second sum on the right-hand side of the above expression for S_1, observe that in order to obtain a final expression of a suitable order for the main term (see (3)), application of Merten's prime number theorem [5, p. 466, Theorem 22.8] introduces an error term of order $O(1/\log P)$, which is of the same order as the main term $\log 2/\log P$ obtained from Merten's theorem for the sum over the range $p\sim P$. Explicitly, from Merten's theorem,

$$\sum_{p\sim P}\frac{1}{p}=\log\left(\frac{\log 2P}{\log P}\right)+O\left(\frac{1}{\log P}\right).$$

Then, by applying the Taylor's series for $\log(1+A)$ to $\log(\log 2P/\log P)$ with $A=\log 2P/\log P-1$ and by noting that $|A|<1$ and that A simplifies to $A=\log 2/\log P$, we obtain the following expression for the main term of the above:

$$\log\left(\frac{\log 2P}{\log P}\right)=\frac{\log 2}{\log P}+O\left(\frac{1}{(\log P)^2}\right),$$

which is of the same order as the error term in Merten's theorem.

Fortunately, however, it is possible to obtain this same main term $\log 2/\log P$ for the sum but with an error term of order $O(1/(\log P)^2)$, by using partial summation as detailed in the following discussion. To proceed, we observe that

$$\int_2^N\frac{1}{\log x}\,dx=\sum_{n=2}^{N}\frac{1}{\log n}+O(1),$$

and we note that any error from the prime number theorem with the logarithmic integral as the main term will be the same as that obtained by using the sum on the right-hand side of the above expression as the main term. Hence, upon using the prime number theorem in the form

$$\sum_{p\leqslant N}1=\sum_{n=2}^{N}\frac{1}{\log n}+O\left(\frac{N}{(\log N)^2}\right),$$

partial summation gives

$$\sum_{p\sim P}\frac{1}{p}=\frac{\log 2}{\log P}\left(1+O\left(\frac{1}{\log P}\right)\right).$$

The argument for this partial summation (see [7, p. 13]) is

$$\begin{aligned}\sum_{p\sim P}\frac{1}{p}&=\sum_{n\sim P}\left(\frac{1}{n}-\frac{1}{n+1}\right)\sum_{P\leqslant p\leqslant n}1+\frac{1}{2P+1}\sum_{p\sim P}1\\&=\sum_{n\sim P}\left(\frac{1}{n}-\frac{1}{n+1}\right)\sum_{P\leqslant m\leqslant n}\frac{1}{\log m}+\frac{1}{2P+1}\sum_{m\sim P}\frac{1}{\log m}+O\left(\frac{1}{(\log P)^2}\right)\\&=\sum_{n\sim P}\frac{1}{n\log n}+O\left(\frac{1}{(\log P)^2}\right)\\&=\frac{\log 2}{\log P}\left(1+O\left(\frac{1}{\log P}\right)\right),\end{aligned}$$

since the third-from-last line in the above is essentially what is obtained upon applying partial summation to the second-from-last line.

https://doi.org/10.1112/S1461157012000058 Published online by Cambridge University Press

Note that although the error term in the prime number theorem can be as small as $O(N\exp(-(\log N)^{\alpha}))$ for $\alpha < 3/5$, the larger error $O(N(\log N)^{-2})$ is sufficient since an error of similar size is introduced in the last line of the partial summation argument above.

Hence we obtain the following estimate for S_1:

$$S_1 = \frac{y(\log 2)^2}{r^2 \log P} + O\left(\frac{y}{r^2(\log P)^2}\right) + O\left(\frac{y}{rN\log P}\right). \tag{5}$$

Next, consider S_2. We use the truncated Fourier series for ψ (see, for example, [7, p. 108]),

$$\psi(x) = -\frac{1}{2\pi i}\sum_{0<|h|<H}\frac{e(hx)}{h} + O\left(\min\left(1, \frac{1}{H\|x\|}\right)\right).$$

We shall use this expression for ψ, take t to be the value of the argument of ψ in S_2, and write $c_h = -1/(2\pi i h)$. As a result of applying this truncated Fourier series, we note that two error terms will be generated for $\psi(t)$ at each value $t = x/n'pr^2$ and $t = (x+y)/n'pr^2$ of its argument. Explicitly, these will be

$$O\left(\sum_{\substack{n'\sim N/r\\ p\sim P}}\min\left(1, \frac{1}{H\|x/n'pr^2\|}\right)\right) + O\left(\sum_{\substack{n'\sim N/r\\ p\sim P}}\min\left(1, \frac{1}{H\|(x+y)/n'pr^2\|}\right)\right).$$

We must choose the larger of these two errors, and for brevity we write it as

$$O\left(\sum_{\substack{n'\sim N/r\\ p\sim P}}\max_{n'pr^2 t = x \text{ or } (x+y)}\min\left(1, \frac{1}{H\|t\|}\right)\right),$$

with the understanding that the maximum is being taken over t and can occur only at either of the two values of the argument t of $\psi(t)$ in S_2. Hence we now write

$$\begin{aligned} S_2 &= \sum_{\substack{n'\sim N/r\\ p\sim P}}\left(\sum_{0<|h|<H} c_h e\left(\frac{hx}{n'pr^2}\right) - \sum_{0<|h|<H} c_h e\left(\frac{h(x+y)}{n'pr^2}\right)\right)\\ &\quad + O\left(\sum_{\substack{n'\sim N/r\\ p\sim P}}\max_{n'pr^2 t = x \text{ or } (x+y)}\min\left(1, \frac{1}{H\|t\|}\right)\right)\\ &= S_3 + S_4, \end{aligned}$$

say. After changing the order of summation, the sum S_3 can be written as

$$S_3 = -\sum_{0<|h|<H}\frac{1}{2\pi i h}\sum_{\substack{n'\sim N/r\\ p\sim P}}\left(e\left(\frac{hx}{n'pr^2}\right) - e\left(\frac{h(x+y)}{n'pr^2}\right)\right).$$

Next, by observing that

$$-\left(e\left(\frac{hx}{n'pr^2}\right) - e\left(\frac{h(x+y)}{n'pr^2}\right)\right) = \frac{2\pi i h}{n'pr^2}\int_x^{x+y} e\left(\frac{Yh}{n'pr^2}\right)dY,$$

we may write

$$S_3 = \int_x^{x+y}\frac{1}{r^2}\sum_{0<|h|<H}\sum_{\substack{n'\sim N/r\\ p\sim P}}\frac{1}{n'p}e\left(\frac{Yh}{n'pr^2}\right)dY.$$

The integrand is the product of $1/r^2$ and the sum

$$\sum_{0<|h|<H}\sum_{\substack{n'\sim N/r\\ p\sim P}}\frac{1}{n'p}e\left(\frac{Yh}{n'pr^2}\right).$$

https://doi.org/10.1112/S1461157012000058 Published online by Cambridge University Press

By applying partial summation to the variable n' (this being over consecutive integers), the coefficient $1/n'$ can now be removed. On performing partial summation (see, for example, [7, p. 13]) we may now re-express the sum as

$$\sum_{\substack{0<|h|<H\\ p\sim P}} \frac{1}{p}\Bigg(\sum_{n'\sim N/r}\left(\frac{1}{n'}-\frac{1}{n'+1}\right)\sum_{N/r\leqslant s\leqslant n'} e\left(\frac{Yh}{spr^2}\right)\Bigg) + \sum_{\substack{0<|h|<H\\ p\sim P}} \frac{1}{p}\Bigg(\frac{1}{[2N/r]+1}\sum_{s\sim N/r} e\left(\frac{Yh}{spr^2}\right)\Bigg).$$

In the above expression we have two exponential sums, one of which is a truncated form of the other. Hence we require a bound for the sum

$$\sum_{0<|h|<H}\sum_{\substack{N/r<n'<S\\ p\sim P}} \frac{1}{p} e\left(\frac{Yh}{n'pr^2}\right) \quad \text{for } S\leqslant 2N/r$$

(where, for clarity, we have replaced the dummy variable s by n', as in the original sum).

We may therefore proceed by obtaining a suitable bound on the above exponential sum over the full non-truncated range $n'\sim N/r$. By this process we essentially reduce the problem of bounding S_3 to demonstrating a non-trivial bound for the sum

$$\sum_{0<|h|<H}\sum_{\substack{n'\sim N/r\\ p\sim P}} \frac{1}{p} e\left(\frac{Yh}{n'pr^2}\right).$$

The variable n' runs over consecutive integers while the variable p runs over primes. We therefore define c_ℓ to be the function

$$c_\ell = \begin{cases} \dfrac{1}{\ell} & \text{if } \ell \text{ is prime,}\\ 0 & \text{otherwise,}\end{cases}$$

and write the sum as

$$\sum_{0<|h|<H}\sum_{\substack{n'\sim N/r\\ \ell\sim P}} c_\ell e\left(\frac{Yh}{n'\ell r^2}\right). \tag{6}$$

This is a type I sum (using the nomenclature of Vaughan) in which the variable n' runs over consecutive integers, and we appeal next to the following lemma (see [8, Section 2] for a proof and how the result we require follows immediately from [8, Corollary 2]).

LEMMA 2. *Let $X>1$ and suppose $X\leqslant\xi<2X$. Suppose $v\in(X^{\frac{1}{2}},X^{\frac{4}{5}}]$ and $K=(v,ev]$. Suppose $m\sim M$ where $X^{\frac{1}{8}}\ll M\ll X^{\frac{2}{5}-\epsilon/2}$, and let $|a_m|\leqslant 1$. Then*

$$\sum_h\sum_{m,n} a_m e\left(\frac{\xi h}{mn}\right)\ll vX^{-2\eta},$$

where $mn\in K$ and $h\leqslant vX^{-\frac{1}{2}+3\eta}$ for some $\eta=\eta(\epsilon)>0$.

To apply this lemma to the type I sum (6), note that we have already seen that we can assume $P>x^{\frac{1}{8}}$. We can then apply the lemma with $X=x/r^2$, $v=NP/r$, $K=(NP/r,eNP/r]$, $\xi=Y/r^2$ and $M=P$. We then have

$$P\leqslant x^{\frac{2}{5}-\epsilon}\ll (x/r^2)^{\frac{2}{5}-\epsilon/2}.$$

https://doi.org/10.1112/S1461157012000058 Published online by Cambridge University Press

All the other conditions are easily checked to be valid. We note that for the sum (6) to satisfy the lemma, we must have $H \leqslant NP(x/r^2)^{-\frac{1}{2}+3\eta} = (vx^{3\eta}/y)r^{1-6\eta}$ for some $\eta = \eta(\epsilon) > 0$. We now have, from this lemma, that

$$\sum_{0<|h|<H} \sum_{\substack{n' \sim N/r \\ \ell \sim P}} c_\ell e\left(\frac{Yh}{n'pr^2}\right) \ll vx^{-2\eta}. \tag{7}$$

We emphasise the importance of the range $H < (vx^{3\eta}/y)r^{1-6\eta}$ in the above discussion, as this will be required in the bound for S_4 in what follows. The bound on the sum S_3 is now readily obtained:

$$S_3 \ll \int_x^{x+y} \frac{1}{r^2} vx^{-2\eta}\, dY = \frac{v}{r^2} x^{-2\eta} \int_x^{x+y} dY = \frac{v}{r^2} yx^{-2\eta} \ll yx^{-2\eta}.$$

In fact, we also find that $S_4 \ll yx^{-\eta}$. This is achieved by choosing $H = vx^{3\eta}/y$ (which is within the allowable range $H < (vx^{3\eta}/y)r^{1-6\eta}$ for the lemma, as detailed in the discussion above) for $x^{\frac{2}{5}} < v < x^{\frac{3}{4}}$ and any $\eta > 0$. To show this, we first appeal to the next lemma [2, pp. 18–21]. Note that for notational convenience the letter ℓ is used in the following lemma and discussion regarding the sum S_4, but it is understood that this ℓ is different from the one used in the previous discussion regarding S_3 and will take a different range of values.

Lemma 3. *Let*

$$\chi(z) = \begin{cases} 1 & \text{if } \|z\| < \delta, \\ 0 & \text{otherwise}, \end{cases}$$

and let L be an integer of size at least δ^{-1}. Then there are coefficients a_ℓ^+ and a_ℓ^-, with $|a_\ell^+| \ll \delta$ and $|a_\ell^-| \ll \delta$, such that

$$2\delta - \frac{1}{L+1} + \sum_{0<|\ell|\leqslant L} a_\ell^- e(\ell z) \leqslant \chi(z) \leqslant 2\delta + \frac{1}{L+1} + \sum_{0<|\ell|\leqslant L} a_\ell^+ e(\ell z)$$

with

$$|a_\ell^{+/-}| \leqslant \min\left(2\delta + \frac{1}{L+1}, \frac{3}{2\ell}\right).$$

Using this lemma, by choosing the upper bound and letting $L = \delta^{-1}$ we see that given $\chi(z)$ as defined in the lemma we have, for $|a_\ell| \ll \delta$,

$$\chi(z) \ll \delta + \sum_{\ell=1}^{\delta^{-1}} a_\ell e(\ell z).$$

(where the plus superscript has been omitted on the understanding that we are dealing with the upper bound). Using this bound and $|a_\ell| \ll \delta$, we observe that if m is a positive integer and $m \sim M$, then given a sequence of real numbers z_m we also have the bound

$$\sum_{\substack{\|z_m\|<\delta \\ m \sim M}} 1 \ll M\delta + \delta \sum_{\ell=1}^{\delta^{-1}} \left| \sum_{m \sim M} e(\ell z_m) \right|. \tag{8}$$

Note the similarity in form of this bound to the Erdős–Turán theorem (see [2, p. 19, Theorem 2.1]), but here we use a constant coefficient δ rather than the harmonic coefficient in the Erdős–Turán theorem. We can employ this bound to estimate the sum S_4 after some suitable rewriting. The approach we take is to majorize the sum over terms $\min(1, 1/H\|t\|)$ in S_4 by comparing the term $1/H\|t\|$ with dyadic blocks of size 2^{-j} for integers j. To achieve this, we introduce a new variable j which takes positive integer values and define $Q := H2^{-j}$.

https://doi.org/10.1112/S1461157012000058 Published online by Cambridge University Press

Let ξ denote either x or $x+y$, the value at which $t=\xi/n'pr^2$ achieves a maximum for the sum S_4 (see the earlier discussion regarding t after (5)). Then for some integer j we have $1/H\|t\| \geqslant Q/H = 2^{-j}$ whenever $\|t\| = \|\xi/n'pr^2\| < 1/Q$. The condition $\|\xi/n'pr^2\| < 1/Q$ therefore enables us to majorize the sum over terms $\min(1, 1/H\|t\|)$ with the most savings. In the following argument, a summation over $Q = H2^{-j}$ is understood to be a summation over all possible values of Q given by integer values of j. Hence we may write

$$\begin{aligned} S_4 &= \sum_{\substack{n'\sim N/r\\ p\sim P}} \max_{n'pr^2 t = x \text{ or } (x+y)} \min\left(1, \frac{1}{H\|t\|}\right) \\ &\leqslant \sum_{\substack{n'\sim N/r\\ p\sim P}} \min\left(1, \frac{1}{H\|\xi/n'pr^2\|}\right) \\ &\leqslant \sum_{Q=H2^{-j}} \sum_{\substack{n'\sim N/r\\ p\sim P, \|\xi/n'pr^2\|\leqslant 1/Q}} \min\left(1, \frac{Q}{H}\right). \end{aligned}$$

We can replace the double sum conditions $n'\sim N/r$ and $p\sim P$ of the inner sum with a single sum condition up to the product of the tops of these ranges, $n \leqslant 4NP/r$ (where now, for notational convenience, we use the variable n in the sum over the combined range). We thereby majorize the previous sum so that it is

$$\leqslant \sum_{Q=H2^{-j}} \sum_{\substack{n\leqslant 4NP/r\\ \|\xi/nr^2\|\leqslant 1/Q}} \min\left(1, \frac{Q}{H}\right).$$

Lemma 3 and the remarks following it, in particular (8), may now be applied to this sum with $z_n = \xi/nr^2$ and $\delta^{-1} = Q$, noting that the minimum function will select $Q/H = 2^{-j}$ by the restriction $\|\xi/nr^2\| < 1/Q$, thus giving the bound

$$\begin{aligned} &\ll \sum_{Q=H2^{-j}} \frac{Q}{H}\left(\frac{NP}{r}\frac{1}{Q} + \frac{1}{Q}\sum_{\ell=1}^{Q}\left|\sum_{n\leqslant 4NP/r} e\left(\frac{\ell\xi}{nr^2}\right)\right|\right) \\ &= \sum_{Q=H2^{-j}} \left(\frac{NP}{Hr} + \frac{1}{H}\sum_{\ell=1}^{Q}\left|\sum_{n\leqslant 4NP/r} e\left(\frac{\ell\xi}{nr^2}\right)\right|\right) \\ &\ll \frac{NP}{H}\frac{\log H}{r} + \frac{1}{H}\sum_{Q=H2^{-j}}\sum_{\ell=1}^{Q}\left|\sum_{n\leqslant 4NP/r} e\left(\frac{\ell\xi}{nr^2}\right)\right|. \end{aligned}$$

The first term of the last line above is $\ll v/H$, since $NP\log H/r = v\log H/r \ll v$. The inner sum of the second term of the last line above is a simple exponential sum and, by the Kusmin–Landau and van der Corput bounds [4, pp. 7–8, Theorems 2.1 and 2.2], is readily shown to be $\ll NP/r < v$ (recall that $v = NP$). We now prove this, beginning by quoting these two theorems as lemmas.

LEMMA 4 (Kusmin–Landau). *If f is continuously differentiable, f' is monotonic and $\|f'\| \geqslant \lambda > 0$ on $I = (a, b]$, then*

$$\sum_{k\in I} e(f(k)) \ll \lambda^{-1}.$$

https://doi.org/10.1112/S1461157012000058 Published online by Cambridge University Press

LEMMA 5 (van der Corput). *Suppose that f is a real-valued function with two continuous derivatives on I. Suppose also that there is some $\lambda > 0$ and some $\alpha \geqslant 1$ such that $\lambda \leqslant |f''| \leqslant \alpha\lambda$ on $I = (a, b]$. Then*

$$\sum_{k\in I} e(f(k)) \ll \alpha|I|\lambda^{\frac{1}{2}} + \lambda^{-\frac{1}{2}}.$$

We take $f(k) = \ell x/kr^2$ (where we recall that this ℓ relates to the discussion and treatment of S_4 and has range $1 \leqslant \ell \leqslant Q$) in the above two lemmas, for which we have chosen (without loss of generality) the value x for ξ. We then obtain

$$\|f'\| \geqslant \frac{\ell x}{n^2r^2} > 0.$$

Thus we use Lemma 4 when $\|f'\| < 1/2$ (that is, when $NPr \gg \ell x$ since f' is of order $\ell x/(NP)^2r^2$) so that the above remains positive. Furthermore,

$$\frac{\ell x}{n^3r^2} < |f''| < 2\alpha\frac{\ell x}{n^3r^2} \quad \text{for any } \alpha \geqslant 1,$$

for which range we use Lemma 5 (which is when $(NPQr)^2 < \ell x/2$).

Hence, by the lemmas for these two ranges (where k of the lemma is now n of the sum under discussion), we obtain the bounds

$$\left|\sum_{n\leqslant 4NP/r} e\left(\frac{\ell\xi}{nr^2}\right)\right| \ll \frac{n^2r^2}{\ell x} < \left(\frac{4NP}{r}\right)^2\frac{r^2}{\ell x} \ll \frac{(NP)^2}{\ell x} = \frac{v^2}{\ell x}.$$

After summing over ℓ as in the original sum under discussion, this is equal to

$$\frac{v^2\log H}{x} \ll v.$$

We also have, for the second range,

$$\begin{aligned}\left|\sum_{n\leqslant 4NP/r} e\left(\frac{\ell\xi}{nr^2}\right)\right| &\ll \alpha\frac{4NP}{r}\left(\frac{\ell x}{n^3r^2}\right)^{\frac{1}{2}} + \left(\frac{n^3r^2}{\ell x}\right)^{\frac{1}{2}} \\ &\ll \frac{NP}{r}\left(\frac{r\ell x}{(NP)^3}\right)^{\frac{1}{2}} + \left(\frac{(NP)^3}{r\ell x}\right)^{\frac{1}{2}}.\end{aligned}$$

After summing over ℓ $(1 \leqslant \ell \leqslant Q)$, the above is $\ll NPx^{-1/16} \ll v$.

Hence we now have

$$S_4 \ll \frac{v}{H} \ll x^{2\eta}\frac{v}{H}.$$

We may now choose $H = vx^{3\eta}/y$ (which is in the allowable range by the discussion following Lemma 2), giving the bound $S_4 \ll yx^{-\eta}$. By virtue of (7) and this bound for S_4, we have

$$S_2 = S_3 + S_4 \ll yx^{-\eta}. \tag{9}$$

5. *Conclusion*

We are now in a position to bring together all the information regarding the sum (2) under investigation and apply it to (1). This original sum may now be decomposed into several sums and their associated error terms:

$$\begin{aligned}\sum_{\substack{mnp\in I\\(m,n)=1,p\nmid m}} 1 &= \sum_r \mu(r) \sum_{m'n'pr^2\in I} 1 - \sum_{\substack{mnp\in I\\(m,n)=1,p|m}} 1 \\ &= \sum_{r\leqslant L} \mu(r)\frac{y(\log 2)^2}{r^2\log P} + O\left(\frac{y(\log x)^2}{L} + x^{\frac{1}{3}+3\epsilon}\right) + E \end{aligned} \tag{10}$$

https://doi.org/10.1112/S1461157012000058 Published online by Cambridge University Press

where

$$E = E_1 + E_2 + E_3 + E_4.$$

The main term arises from the main term of S_1 in (5), and E_1 is the error resulting from this approximation. The second term of (10) is the bound obtained for larger common factors in (5). The term E_2 comes from the error in reducing to exponential sums (this is essentially S_4, and is observed to become smaller as the range of h increases). The third error term E_3 arises from the estimation of the exponential sum (this being essentially S_3). However, by (9) we have that $E_2 + E_3 \ll yx^{-\eta}$. The fourth term E_4 is the error arising from the case where p divides m, treated in Section 3, which was shown to be $\ll x^{\frac{2}{5}} + yx^{\epsilon-\frac{1}{8}}$. Hence it remains to calculate E_1 and show that this is smaller than the main term.

From (5) we have

$$\begin{aligned} E_1 &= \sum_{r\leqslant L}\left(O\left(\frac{y}{r^2(\log P)^2}\right) + O\left(\frac{y}{rN\log P}\right)\right) \\ &= O\left(\frac{y}{(\log P)^2}\sum_{r\leqslant L}\frac{1}{r^2}\right) + O\left(\frac{y}{N\log P}\sum_{r\leqslant L}\frac{1}{r}\right). \end{aligned}$$

Hence

$$E_1 = O\left(\frac{y}{(\log P)^2}\right) + O\left(\frac{y\log\log x}{N\log P}\right),$$

where the summation over r in the second term has introduced an extra factor $O(\log L) = O(\log\log x)$.

Since by hypothesis $P > 2N > x^{\epsilon}$, we have

$$E_1 = O\left(\frac{y}{(\log x)^2}\right) + O\left(\frac{y\log\log x}{x^{\epsilon}\log x}\right).$$

Hence

$$E_1 \ll \frac{y}{(\log x)^2}.$$

The sum over larger common factors $r > L$ in the second term of (10) was shown to be $\ll y(\log x)^2/L + x^{\frac{1}{3}+3\epsilon}$ (see Section 2).

Also, as P and $\log P$ are no larger than $x^{\frac{3}{4}}$ and $\log x$, respectively, the main term given by the first term of (10) is

$$\sum_{r\leqslant L}\mu(r)\frac{y(\log 2)^2}{r^2\log P} = \frac{y(\log 2)^2}{\log P}\sum_{r\leqslant L}\frac{\mu(r)}{r^2} \gg \frac{y}{\log x}, \tag{11}$$

since the sum is finite.

From (10) we may then conclude that

$$\begin{aligned} \sum_{\substack{mnp\in I\\(m,n)=1,p\nmid m}} 1 &= \sum_{r\leqslant L}\mu(r)\frac{y(\log 2)^2}{r^2\log P} \\ &\quad + O\left(\frac{y(\log x)^2}{L} + x^{\frac{1}{3}+3\epsilon} + \frac{y}{(\log x)^2} + \frac{y}{x^{\eta}} + x^{\frac{2}{5}} + yx^{\epsilon-\frac{1}{8}}\right). \end{aligned}$$

Since $L = (\log x)^A$ (see Section 2), we can therefore choose $A = 4$, giving $L = (\log x)^4$ and thus producing the anticipated error term in (3). Hence, for sufficiently large x, the error term E_1 is a power of $\log x$ smaller than the main term (11), while E_2, E_3 and E_4 are a power of x smaller than the main term. Furthermore, the upper bound obtained in (4) suffices for larger common factors (the second term of (10)). We have therefore established Theorem 1.

https://doi.org/10.1112/S1461157012000058 Published online by Cambridge University Press

The corollary follows immediately from Theorem 1, since for $n \sim N$ and $p \sim P$ and given that $n < p$ with N and P about $x^{\frac{1}{3}}$ in size, we have $P < 2x^{\frac{1}{3}} < x^{\frac{2}{5}-\epsilon}$ with $NP \approx x^{\frac{2}{3}} \leqslant x^{\frac{3}{4}}$, which satisfies the conditions of Theorem 1.

The asymptotic value of the main term is given by

$$\sum_{r \leqslant L} \mu(r) \frac{y(\log 2)^2}{r^2 \log P} = \frac{y(\log 2)^2}{\log P} \sum_{r \leqslant L} \frac{\mu(r)}{r^2} = \frac{6y(\log 2)^2}{\pi^2 \log P}(1 + o(1)).$$

In particular, there are integers of the form required in the corollary within the interval $(x, x + x^{\frac{1}{2}}]$, and the number of such integers is

$$\frac{6y(\log 2)^2}{\pi^2 \log P}(1 + o(1)).$$

References

1. R. C. Baker, 'The greatest prime factor of the integers in an interval', *Acta Arith.* 47 (1986) 193–231.
2. R. C. Baker, *Diophantine inequalities*, London Mathematical Society Monographs (New Series) I (Clarendon Press, Oxford, 1986).
3. K Bentahar, 'The equivalence between the DHP and DLP for elliptic curves used in practical applications, revisited', *Cryptography and coding: 10th IMA international conference, 2005*, Lecture Notes in Computational Science 3796 (Springer, Berlin, 2005) 376–391.
4. S. W. Graham and G. Kolesnik, *Van der Corput's method of exponential sums*, London Mathematical Society Lecture Note Series 126 (Cambridge University Press, Cambridge, 1991).
5. G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers*, 6th edn (Oxford University Press, Oxford, 2008).
6. G. Harman, 'Integers without large prime factors in short intervals and arithmetic progressions', *Acta Arith.* 91 (1999) 279–289.
7. G. Harman, *Prime-detecting sieves*, London Mathematical Society Monographs 33 (Princeton University Press, Princeton, NJ, 2007).
8. H. Q. Liu and J. Wu, 'Numbers with a large prime factor', *Acta Arith.* 89 (1999) 163–187.
9. A. Muzereau, N. P. Smart and F. Vercauteren, 'The equivalence betwen the DHP and DLP for elliptic curves used in practical applications', *LMS J. Comput. Math.* 7 (2004) 50–72.
10. P. Shiu, 'A Brun-Titchmarsh theorem for multiplicative functions', *J. Reine Angew. Math.* 313 (1980) 161–170.

Asim Islam
Department of Mathematics
Royal Holloway, University of London
Egham, Surrey TW20 0EX
United Kingdom

Asim.Islam@rhul.ac.uk

https://doi.org/10.1112/S1461157012000058 Published online by Cambridge University Press