NEW ZEALAND JOURNAL OF MATHEMATICS
Volume 50 (2020), 93–99

ON PRODUCTS OF PRIMES AND SQUARE-FREE INTEGERS IN ARITHMETIC PROGRESSIONS

Kam Hung Yau

(Received 12 August, 2019)

Abstract. We obtain an asymptotic formula for the number of ways to represent every reduced residue class as a product of a prime and square-free integer. This may be considered as a relaxed version of a conjecture of Erdös, Odlyzko, and Sárközy.

1. Introduction

A conjecture of Erdös, Odlyzko, and Sárközy [4] asks if for every reduced residue class a modulo m can be represented as a product

$$p_1p_2 \equiv a \,(\text{mod } m) \tag{1.1}$$

for two primes $p_1, p_2 \leq m$. Friedlander, Kurlberg, and Shparlinski [7] considered an average of (1.1) over a and m, and also various modification of (1.1). Garaev [8, 9] improved on these modifications. Other interesting variants of (1.1) had also been considered by Baker [1], Ramaré & Walker [12], Shparlinski [13, 14], Walker [15].

In this paper, we are concerned with bounding the quantity

$$\#\left\{(p,s) : ps \equiv a \,(\text{mod } q), p \leq P, s \leq S, \mu^2(s) = 1, (ps,q) = 1\right\}$$

for $(a,q) = 1$. This may also be viewed as a multiplicative analogue in the setting of finite fields of a result of Estermann [5]. Estermann [5] showed that all sufficiently large positive integer can be written as a sum of a prime and a square-free integer, see also [10, 11]. Recently, Dudek [3] showed that this is true for all positive integer greater than two.

Our method uses the nice factoring property of the characteristic function for square-free integers

$$\mu^2(n) = \sum_{d^2|n} \mu(d), \tag{1.2}$$

together with bounds for Kloosterman sums over primes supplied by Fourvy and Shparlinski [6], extending those previous result of Garaev [8].

2. Notation

The notation $U = O(V)$ is abbreviated to $U \ll V$, i.e., there exists an absolute constant $C > 0$ such that $U \leq CV$. Throughout this paper p a prime number, μ is the Möbius function, $\tau(n)$ is the number of positive divisors of n and $\varphi(n)$ is the number of positive integers up to n coprime to n.

2010 *Mathematics Subject Classification* 11L05, 11A07.
Key words and phrases: Kloosterman sums, congruences.

3. Result

We denote

$$\pi_q(P) = \#\{p \le P : (p,q) = 1\}$$

to be the number of primes up to P coprime to q, and

$$s_q(S) = \#\{s \le S : \mu^2(s) = 1, (s,q) = 1\}$$

to be the number of square-free integers up to S coprime to q. For $(a,q) = 1$, denote $\mathcal{N}^{\#}_{a,q}(P,S)$ by the quantity

$$\#\left\{(p,s) : ps \equiv a \,(\mathrm{mod}\; q), p \le P, s \le S, \mu^2(s) = 1, (ps,q) = 1\right\}.$$

Theorem 3.1. *For all fixed $A, \varepsilon > 0$, we have*

$$\mathcal{N}^{\#}_{a,q}(P,S) = \frac{\pi_q(P)s_q(S)}{q} + O\left((PS)^{o(1)}S^{1/2}E\right)$$

uniformly for $q \le P^{O(1)}$ and $(a,q) = 1$, where

$$E = \begin{cases} Pq^{-1} & \text{if } q \le (\log P)^A, \\ \dfrac{P}{q^{3/4}} + \dfrac{P^{9/10}}{q^{3/8}} & \text{if } (\log P)^A < q < P^{3/4}, \\ \dfrac{P^{31/32}}{q^{(1-\varepsilon)/2}} + \dfrac{P^{5/6}}{q^{(3/4-\varepsilon)/2}} & \text{if } P^{3/4} \le q. \end{cases}$$

The main term in Theorem 3.1 is

$$\begin{aligned} \frac{\pi_q(P)s_q(S)}{q} &\gg \frac{1}{q}\frac{P}{\log P}\left(\frac{\varphi(q)S}{q} + O(\tau(q))\right) \\ &\gg P^{1+o(1)}Sq^{-1} \end{aligned}$$

since $q \le P^{O(1)}$. It follows that $\mathcal{N}^{\#}_{a,q}(P,S) > 0$ when $P \to \infty$ if either one of the following three conditions below holds.

(1) $q \le (\log P)^A$ and there exists an $\varepsilon > 0$ such that $S \gg P^{\varepsilon}$.

(2) $(\log P)^A < q < P^{3/4}$ and there exists an $\varepsilon > 0$ such that

$$S^2 \gg (PS)^{\varepsilon} q \qquad \text{and} \qquad P^4 S^{20} \gg (PS)^{\varepsilon} q^{25}.$$

(3) $P^{3/4} \le q$ and there exists an $\varepsilon > 0$ such that

$$PS^{16} \gg (PS)^{\varepsilon} q^{16} \qquad \text{and} \qquad P^4 S^{12} \gg (PS)^{\varepsilon} q^{15}.$$

4. Preliminaries

For $(a,q) = 1$, we denote the Kloosterman sum over primes

$$S_q(a;x) = \sum_{\substack{p \le x \\ (p,q)=1}} \mathbf{e}_q(a\bar{p}).$$

Here $\mathbf{e}_q(x) = \exp(2\pi i x/q)$ and $\bar{p}$ is the multiplicative inverse for p modulo q. Bounds for when q is a prime had been obtained by Garaev [8]. Fouvry and Shparlinski [6] extended these results for composite q. We gather Theorem 3.1, 3.2 and (3.13) from [6] into the following lemma.

Lemma 4.1. *For every fixed $A, \varepsilon > 0$, we have*

$$S_q(a;x) = O(B_q(x)),$$

uniformly for integer $q \geq 2$, $(a,q) = 1$ and $x \geq 2$. Here

$$B_q(x) = \begin{cases} x^{1+o(1)}q^{-1} & \text{if } q \leq (\log x)^A, \\ (q^{-1/2}x + q^{1/4}x^{4/5})x^{o(1)} & \text{if } (\log x)^A < q < x^{3/4}, \\ (x^{15/16} + q^{1/4}x^{2/3})q^{\varepsilon} & \text{if } x^{3/4} \leq q. \end{cases}$$

Denote

$$\mathcal{N}_{a,q}(P,S) = \#\left\{(p,s) : ps \equiv a \,(\mathrm{mod}\ q), p \leq P, s \leq S, (ps,q) = 1\right\}$$

for $(a,q) = 1$. Below we provide an upper bounds for $\mathcal{N}_{a,q}(P,S)$.

Lemma 4.2. *For $q \leq P^{O(1)}$, we have*

$$\mathcal{N}_{a,q}(P,S) \ll \left(\frac{PS}{q} + 1\right)(PS)^{o(1)}.$$

Proof. By counting the number of solutions to $ps = a + kq$. we obtain the bound $k \ll (PS/q + 1)$. For each $a + kq$, the number of distinct prime factors is no more than

$$\ll \log(kq) \ll \log(PS + q) \ll \log(PS) \ll (PS)^{o(1)},$$

from our upper bound on k. □

Denote

$$N_q(P,S) = \#\{(p,s) : p \leq P, s \leq S, (ps,q) = 1\}.$$

We relate the quantity $\mathcal{N}_{a,q}(P,S)$ with $N_q(P,S)$.

Lemma 4.3. *For all fixed $\varepsilon > 0$, we have*

$$\mathcal{N}_{a,q}(P,S) = \frac{N_q(P,S)}{q} + O(B_q(P)),$$

uniformly for $(a,q) = 1$, where B_q is defined as in Lemma 4.1.

Proof. We interpret this as a uniform distribution problem. Namely we consider

$$s \equiv a\bar{p} \pmod q$$

which fall in the interval $[1,S]$. The result follows from Lemma 4.1 applied with the Erdös-Turán inequality, see [**2**]. □

Now we can provide a bound for $N_q(P,S)$.

Lemma 4.4. *For $q \leq P^{O(1)}$, we have*

$$N_q(P,S) = \frac{\varphi(q)\pi_q(P)S}{q} + O(P^{1+o(1)}).$$

Proof. Note the identity

$$\sum_{d|n} \mu(d) = \begin{cases} 1 & \text{if } n = 1, \\ 0 & \text{otherwise.} \end{cases}$$

We have

$$\begin{aligned} N_q(P,S) &= \sum_{\substack{p \le P \\ (p,q)=1}} 1 \sum_{\substack{s \le S \\ (s,q)=1}} 1 \\ &= \pi_q(P) \sum_{s \le S} \sum_{\substack{d|s \\ d|q}} \mu(d) \\ &= \pi_q(P) \left(\frac{\varphi(q) S}{q} + O(\tau(q)) \right) \\ &= \frac{\varphi(q) \pi_q(P) S}{q} + O(P^{1+o(1)}). \end{aligned}$$

□

We also provide a bound for $s_q(S)$.

Lemma 4.5. *We have*

$$s_q(S) = \frac{\varphi(q)}{q} \prod_{p \nmid q} \left(1 - \frac{1}{p^2}\right) S + O(S^{1/2} q^{o(1)}).$$

Proof. We first expand $s_q(S)$:

$$\begin{aligned} s_q(S) &= \sum_{\substack{d \le S^{1/2} \\ (d,q)=1}} \mu(d) \sum_{\substack{s \le S/d^2 \\ (s,q)=1}} 1 \\ &= \sum_{\substack{d \le S^{1/2} \\ (d,q)=1}} \mu(d) \sum_{s \le S/d^2} \sum_{\substack{r|s \\ r|q}} \mu(r). \end{aligned}$$

Interchanging summation and completing the series, we get

$$\begin{aligned} s_q(S) &= \sum_{r|q} \mu(r) \sum_{\substack{d \le S^{1/2} \\ (d,q)=1}} \mu(d) \left(\frac{S}{d^2 r} + O(1) \right) \\ &= \frac{\varphi(q)}{q} \left(\sum_{\substack{d=1 \\ (d,q)=1}}^{\infty} \frac{\mu(d)}{d^2} - \sum_{\substack{d > S^{1/2} \\ (d,q)=1}} \frac{\mu(d)}{d^2} \right) S + O(S^{1/2} \tau(q)) \\ &= \frac{\varphi(q)}{q} \prod_{p \nmid q} \left(1 - \frac{1}{p^2}\right) S + O(S^{1/2} q^{o(1)}). \end{aligned}$$

Note that we used the below equality:

$$\varphi(q) = q \prod_{p|q} \left(1 - \frac{1}{q}\right) = q \sum_{r|q} \frac{\mu(r)}{r}.$$

□

5. Proof of Theorem 3.1

Using (1.2), we obtain

$$\begin{aligned}
\mathcal{N}^{\#}_{a,q}(P,S) &= \sum_{\substack{p\le P \\ ps\equiv a \pmod q,\, (ps,q)=1}} \sum_{s\le S} \mu^2(s) \\
&= \sum_{\substack{d\le S^{1/2} \\ (d,q)=1}} \mu(d)\mathcal{N}_{ad^{-2},q}(P,S/d^2) \\
&= \Sigma_1+\Sigma_2,
\end{aligned}$$

where

$$\Sigma_1 = \sum_{\substack{d\le D \\ (d,q)=1}} \mu(d)\mathcal{N}_{ad^{-2},q}(P,S/d^2),$$

and

$$\Sigma_2 = \sum_{\substack{D<d\le S^{1/2} \\ (d,q)=1}} \mu(d)\mathcal{N}_{ad^{-2},q}(P,S/d^2).$$

Here $D=D(P,S)$ is a parameter that will be chosen later.

We bound Σ_2 by Lemma 4.2:

$$\begin{aligned}
\Sigma_2 &\ll \sum_{D<d\le S^{1/2}} \left(\frac{PS}{d^2q}+1\right)\left(\frac{PS}{d^2}\right)^{o(1)} \\
&\ll (PS)^{o(1)}\left(\frac{PS}{qD}+S^{1/2}\right).
\end{aligned}$$

Using Lemma 4.3 and 4.4 we get

$$\begin{aligned}
\Sigma_1 &= \sum_{\substack{d\le D \\ (d,q)=1}} \mu(d)\left(\frac{N_q(P,S/d^2)}{q}+O(B_q(P))\right) \\
&= \sum_{\substack{d\le D \\ (d,q)=1}} \mu(d)\left(\frac{\varphi(q)\pi_q(P)S}{q^2d^2}+O(P^{1+o(1)}q^{-1})\right)+O(DB_q(P)).
\end{aligned}$$

Completing the series in the summation over d, we assert that

$$\begin{aligned}\Sigma_1 &= \frac{\varphi(q)\pi_q(P)S}{q^2}\left(\sum_{\substack{d=1\\(d,q)=1}}^{\infty}\frac{\mu(d)}{d^2}-\sum_{\substack{d>D\\(d,q)=1}}\frac{\mu(d)}{d^2}\right)\\ &\quad + O(D\{B_q(P)+P^{1+o(1)}q^{-1}\})\\ &= \frac{\pi_q(P)}{q}\left(\frac{\varphi(q)S}{q}\sum_{\substack{d=1\\(d,q)=1}}^{\infty}\frac{\mu(d)}{d^2}\right)+O\left(\frac{PS}{qD}+DB_q(P)\right)\\ &= \frac{\pi_q(P)s_q(S)}{q}+O\left(\frac{S^{1/2}\pi_q(P)}{q^{1+o(1)}}+\frac{PS}{qD}+DB_q(P)\right),\end{aligned} \tag{5.1}$$

where the last line follows from Lemma 4.5.

Now we set

$$D=\begin{cases} S^{1/2}P^{o(1)} & \text{if } q\le(\log P)^A,\\ \left(\dfrac{PS}{Pq^{1/2}+q^{5/4}P^{4/5}}\right)^{1/2}P^{o(1)} & \text{if } (\log P)^A<q<P^{3/4},\\ \left(\dfrac{PS}{q^{1+\varepsilon}(P^{15/16}+q^{1/4}P^{2/3})}\right)^{1/2} & \text{if } P^{3/4}\le q.\end{cases}$$

Then the last two terms in (5.1) are equal and it follows that

$$\mathcal{N}^{\#}_{a,q}(P,S)=\frac{\pi_q(P)s_q(S)}{q}+O\left(\left(\frac{S^{1/2}\pi_q(P)}{q^{1+o(1)}}+\frac{PS}{qD}+S^{1/2}\right)(PS)^{o(1)}\right).$$

If $q\le(\log P)^A$ then the error term above is majorised by

$$\left(\frac{PS^{1/2}}{q}+S^{1/2}\right)(PS)^{o(1)}\ll PS^{1/2}q^{-1}(PS)^{o(1)}.$$

If $(\log P)^A<q<P^{3/4}$ then the error term above is majorised by

$$\begin{aligned}&\left(\frac{P^{1/2}S^{1/2}(Pq^{1/2}+q^{5/4}P^{4/5})^{1/2}}{q}+S^{1/2}\right)(PS)^{o(1)}\\ &\qquad\ll S^{1/2}\left(\frac{P}{q^{3/4}}+\frac{P^{9/10}}{q^{3/8}}\right)(PS)^{o(1)}.\end{aligned}$$

Lastly, if $P^{3/4}\le q$ then the error term above is majorised by

$$\begin{aligned}&\left(\frac{P^{1/2}S^{1/2}(q^{1+\varepsilon}\{P^{15/16}+q^{1/4}P^{2/3}\})^{1/2}}{q}+S^{1/2}\right)(PS)^{o(1)}\\ &\qquad\ll S^{1/2}\left(\frac{P^{31/32}}{q^{(1-\varepsilon)/2}}+\frac{P^{5/6}}{q^{(3/4-\varepsilon)/2}}\right)(PS)^{o(1)}.\end{aligned}$$

So the result follows.

Acknowledgement

The author thanks I. E. Shparlinski for the problem and helpful comments together with Liangyi Zhao. The author also thanks the referee for helpful comments. This work is supported by an Australian Government Research Training Program (RTP) Scholarship.

References

[1] R. C. Baker, *Kloosterman sums with prime variable,* Acta Arith. **156** (4) (2012), 351–372.

[2] M. Drmota and R. F. Tichy, *Sequences, Discrepancies and Applications,* Lecture Notes in Mathematics 1651, Springer, Berlin, 1997.

[3] A. W. Dudek, *On the sum of a prime and a square-free number,* Ramanujan J. **42** (1) (2017), 233–240.

[4] P. Erdös, A. M. Odlyzko, A. Sárközy, *On the residues of products of prime numbers,* Period. Math. Hung. **18** (1987), 229–239.

[5] T. Estermann, *On the Representations of a number as the sum of a prime and a quadratfrei number,* J. Lond. Math. Soc. **6** (1931), 219–221.

[6] E. Fouvry, I. E. Shparlinski, *On a ternary quadratic form over primes,* Acta Arith. **150** (3) (2011), 285–314.

[7] J. B. Friedlander, P. Kurlberg, I. E. Shparlinski, *Products in residue classes,* Math. Res. Lett. **15** (5–6) (2008), 1133–1147.

[8] M. Z. Garaev, *Estimation of Kloosterman sums with primes and its application,* Mat. Zametki **88** (3) (2010), 533–541 (in Russian).

[9] M. Z. Garaev, *On multiplicative congruences,* Math. Z. **272** (1–2) (2012), 473–482.

[10] L. Mirsky, *The number of representations of an integer as the sum of a prime and a k-free integer.* Am. Math. Mon. **56** (1949), 17–19.

[11] A. Page, *On the number of primes in an arithmetic progression.* Proc. London Math. Soc. II **39** (2) (1935), 116–141.

[12] O. Ramaré, A. Walker, *Products of primes in arithmetic progressions: a footnote in parity breaking,* J. Théor. Nombres Bordx. **30** (1) (2018), 219–225.

[13] I. E. Shparlinski, *On products of primes and almost primes in arithmetic progressions,* Period. Math. Hung. **67** (1) (2013), 55–61.

[14] I. E. Shparlinski, *On short products of primes in arithmetic progressions,* Proc. Am. Math. Soc. **147** (3) (2019), 977–986.

[15] A. Walker, *A multiplicative analogue of Schnirelmann's theorem,* Bull. Lond. Math. Soc. **48** (6) (2016), 1018–1028.

Kam Hung Yau
Department of Pure
Mathematics,
University of New South
Wales,
Sydney,
NSW 2052,
Australia
kamhungyau.math@gmail.com