INCOMPLETE KLOOSTERMAN SUMS AND MULTIPLICATIVE INVERSES IN SHORT INTERVALS

T. D. BROWNING AND A. HAYNES

Abstract. We investigate the solubility of the congruence $xy \equiv 1 \pmod{p}$, where $p$ is a prime and $x, y$ are restricted to lie in suitable short intervals. Our work relies on a mean value theorem for incomplete Kloosterman sums.

1. Introduction

Let $p$ be a prime, and let $I_1, I_2 \subseteq (0, p)$ be subintervals. This paper is motivated by determining conditions on $I_1, I_2$ under which we can ensure the solubility of the congruence $xy \equiv 1 \pmod{p}, \ (x, y) \in I_1 \times I_2$.

From a heuristic point of view we would expect this congruence to have a solution whenever $|I_1|, |I_2| \gg p^{1/2}$. However, as highlighted by Heath-Brown [2], the best result to date requires that $|I_1| \cdot |I_2| \gg p^{3/2} \log^2 p$. The proof requires one to estimate incomplete Kloosterman sums

$$S(n, H) = \sum_{m=n+1}^{n+H} e\left(\frac{\ell m}{p}\right),$$

for $\ell \in (\mathbb{Z}/\ell\mathbb{Z})^*$, for which the Weil bound yields

$$|S(n, H)| \leq 2(1 + \log p)p^{1/2}. \quad (1)$$

It has been conjectured by Hooley [4] that $S(n, H) \ll H^{1/2} q^\varepsilon$, for any $\varepsilon > 0$, which would enable one to handle intervals with $|I_1|, |I_2| \gg p^{2/3+\varepsilon}$. However such a bound appears to remain a distant prospect.

A different approach to this problem involves considering a sequence of pairs of intervals $I_1^{(j)}, I_2^{(j)}$, for $1 \leq j \leq J$, and to ask whether there is a value of $j$ for which there is a solution to the congruence

$$xy \equiv 1 \pmod{p}, \ (x, y) \in I_1^{(j)} \times I_2^{(j)}. \quad (2)$$

There are some obvious degenerate cases here. For example, if we suppose that $I_1^{(j)} = I_2^{(j)}$ for all $j$, and that these run over all intervals of a given length $H$, then we are merely asking whether there is positive integer $h \leq H$ with the property that the congruence $x(x + h) \equiv 1 \pmod{p}$ has a solution $x \in \mathbb{Z}$. This is equivalent to deciding whether the set $\{h^2 + 4 : 1 \leq h \leq H\}$ contains a quadratic residue modulo $p$. When $H = 2$, therefore, it is clear that this problem has a solution for all primes $p = \pm 1 \pmod{8}$. We avoid...
considerations of this sort by assuming that at least one of our sequences of intervals is pairwise disjoint. The following is our main result.

**Theorem 1.** Let $H, K > 0$ and let $I_1^{(j)}, I_2^{(j)} \subseteq (0, p)$ be subintervals, for $1 \leq j \leq J$, such that

$$|I_1^{(j)}| = H \quad \text{and} \quad |I_2^{(j)}| = K$$

and

$$I_1^{(j)} \cap I_1^{(k)} = \emptyset \quad \text{for all} \quad j \neq k.$$ 

Then there exists $j \in \{1, \ldots, J\}$ for which $\text{(2)}$ has a solution if

$$J \gg \frac{p^3 \log^4 p}{H^2 K^2}.$$ 

If we take $J = 1$ in the theorem then we retrieve the above result that $\text{(2)}$ is soluble when $HK \gg p^{5/2} \log^2 p$. Alternatively, if we allow a larger value of $J$, then we can get closer to what would follow on Hooley’s hypothesised bound for $S(n, H)$.

**Corollary.** With notation as in Theorem 1, suppose that $J \gg p^{1/3}$. Then there exists $j \in \{1, \ldots, J\}$ for which $\text{(2)}$ has a solution provided that $H > p^{2/3}$ and $K > p^{2/3} (\log p)^2$.

Our proof of Theorem 1 relies upon a mean value estimate for incomplete Kloosterman sums. These types of estimates have been studied extensively for multiplicative characters, especially in connection with variants of Burgess’s bounds (see Heath-Brown [3] and the discussion therein). The situation for Kloosterman sums is relatively under-developed (see Friedlander and Iwaniec [1], for example). The result we present here appears to be new, although many of our techniques are borrowed directly from the treatment of the analogous multiplicative problem [3, Theorem 2]. The deepest part of our argument is an appeal to Weil’s bound for Kloosterman sums. We will prove the following result in the next section.

**Theorem 2.** If $I_1, \ldots, I_J \subseteq (0, p)$ are disjoint subintervals, with $H/2 < |I_j| \leq H$ for each $j$, then for any $\ell \in (\mathbb{Z}/p\mathbb{Z})^*$, we have

$$\sum_{j=1}^J \left| \sum_{n \in I_j} e\left(\frac{\ell n}{p}\right) \right|^2 \leq 2^{12} p \log^2 H.$$ 

Taking $J = 1$ shows that, up to a constant factor, this result includes as a special case the bound (1) for incomplete Kloosterman sums.

**Acknowledgements.** While working on this paper TDB was supported by EPSRC grant EP/E053262/1 and AH was supported by EPSRC grant EP/J00149X/1. We are grateful to Professor Heath-Brown for several useful discussions.

2. **Proof of Theorem 2**

Our starting point is the following mean value theorem for $S(n, H)$.
Lemma. For $H \in \mathbb{N}$ and $\ell \in (\mathbb{Z}/p\mathbb{Z})^*$, we have

$$\sum_{n=1}^{p} |S(n, H)|^2 \leq \frac{H^2}{p} + 8pH.$$ 

Proof. After squaring out the inner sum and interchanging the order of summation, the left hand side becomes

$$\sum_{h_1, h_2=1}^{H} \sum_{n=1}^{p} e \left( \frac{\ell(n + h_1 - n + h_2)}{p} \right).$$

Using orthogonality of characters it is easy to see that the inner sum over $n$ is

$$= \sum_{x, y \in (\mathbb{Z}/p\mathbb{Z})^*} e \left( \frac{\ell(x - y)}{p} \right) \sum_{h_1, h_2=1}^{H} e \left( \frac{a(h_2 - h_1)}{p} \right),$$

where $K(\ell, a; p)$ is the usual complete Kloosterman sum. The contribution from $a = p$ is

$$\left| K(\ell, 0; p) \right|^2 \frac{H^2}{p} = \frac{H^2}{p},$$

since $p \nmid \ell$. The remaining contribution has modulus

$$\left| \frac{1}{p} \sum_{a=1}^{p-1} |K(\ell, a; p)|^2 \sum_{h_1, h_2=1}^{H} e \left( \frac{a(h_2 - h_1)}{p} \right) \right| \leq 8 \sum_{0 < a < p/2} \min \left\{ H, \frac{p}{2a} \right\}^2 \leq 8pH,$$

by the Weil bound for the Kloosterman sum and the familiar estimate for a geometric series. Combining these contributions, we therefore arrive at the statement of the lemma. \qed

The rest of the proof of Theorem 2 is taken from the proof of [3, Theorem 2], and we include it only for completeness. We may assume that $H \geq 4$ in what follows since the result is trivial otherwise. Write $N_j$ for the smallest integer in $I_j$ and suppose that
By separately considering the odd and then the even numbered intervals we may assume without loss of generality that $N_{j+1} - N_j \geq H$ for $1 \leq j < J$.

The starting point is the observation that

$$
\sum_{j=1}^{J} \sum_{n \in I_j} e \left( \frac{\ell n}{p} \right) \leq \sum_{j=1}^{J} \max_{1 \leq h \leq H} |S(N_j, h)|^2.
$$

(3)

For any $1 \leq h \leq H$ and $N_j - H < n \leq N_j$ we have that

$$
|S(N_j, h)| = |S(n, N_j - n + h) - S(n, N_j - n)| \leq 2 \max_{1 \leq k \leq 2H} |S(n, k)|,
$$

whence

$$
|S(N_j, h)| \leq \frac{2}{H} \sum_{N_j-H<n\leq N_j} \max_{1 \leq k \leq 2H} |S(n, k)|.
$$

Cauchy’s inequality yields

$$
|S(N_j, h)|^2 \leq \frac{4}{H} \sum_{N_j-H<n\leq N_j} \max_{1 \leq k \leq 2H} |S(n, k)|^2.
$$

Taking the max over $h$ and then summing over $j$ now gives

$$
\sum_{j=1}^{J} \max_{1 \leq h \leq H} |S(N_j, h)|^2 \leq \frac{4}{H} \sum_{j=1}^{J} \sum_{N_j-H<n\leq N_j} \max_{1 \leq k \leq 2H} |S(n, k)|^2
$$

$$
\leq \frac{4}{H} \sum_{n=1}^{p} \max_{1 \leq k \leq 2H} |S(n, k)|^2,
$$

(4)

the last inequality coming from our spacing assumption. We now seek an upper bound for the sum on the right hand side.

Let $t$ be the smallest positive integer with $2H \leq 2^t$, so that in particular $2H \leq 2^t \leq 4H$ and $t+1 \leq 4 \log H$. For each $1 \leq n \leq p$ we choose a positive integer $k = k(n) \leq 2H$, with

$$
\max_{1 \leq h \leq 2H} |S(n, h)| = |S(n, k)|.
$$

By writing $k = \sum_{d \in \mathcal{D}} 2^{t-d}$, where $\mathcal{D}$ is a collection of integers in $[0, t]$, we have that

$$
S(n, k) = \sum_{d \in \mathcal{D}} S(n + v_{n,d} 2^{t-d}, 2^{t-d}),
$$

where

$$
v_{n,d} = \sum_{e \in \mathcal{D}, e<d} 2^{d-e} < 2^d.
$$
Then by Cauchy’s inequality we deduce that
\[
\max_{1 \leq h \leq 2H} |S(n, h)|^2 \leq |\mathcal{P}| \sum_{d \in \mathcal{P}} |S(n + v_{n,d}2^{t-d}, 2^{t-d})|^2
\leq (t + 1) \sum_{0 \leq d \leq t} \sum_{0 \leq v < 2^d} |S(n + v2^{t-d}, 2^{t-d})|^2.
\]
Now summing both sides over \(n\) and applying Lemma 2 we have that
\[
\sum_{n=1}^p \max_{1 \leq k \leq 2H} |S(n, k)|^2 \leq (t + 1) \sum_{0 \leq d \leq t} \sum_{0 \leq v < 2^d} \left( \frac{2^{2t-2d}}{p} + 8p^{2t-d} \right)
\leq (t + 1)^2 \left( \frac{2^{2t}}{p} + 8p^2 \right)
\leq 2^8 \left( \frac{H^2}{p} + 2pH \right) \log^2 H.
\]
Since \(H^2/p \leq 2pH\) we easily complete the proof of Theorem 2 by combining this with (3) and (4).

3. Proof of Theorem 1

Now we proceed to the proof of our main theorem. For each \(j\) the number of solutions to (2) is equal to
\[
\sum_{x \in I_1^{(j)}, y \in I_2^{(j)}} \frac{1}{p} \sum_{\ell=1}^p e \left( \frac{\ell(x - y)}{p} \right) = \sum_{x \in I_1^{(j)}, y \in I_2^{(j)}} \frac{1}{p} \sum_{\ell=1}^p \sum_{x \in I_1^{(j)}, y \in I_2^{(j)}} e \left( \frac{\ell(x - y)}{p} \right) = S_{1,j} + S_{2,j},
\]
say. The total contribution from the \(S_{1,j}\) terms is
\[
\sum_{j=1}^J S_{1,j} \gg \frac{JHK}{p}.
\]
Next, the standard estimate for a geometric series gives
\[
S_{2,j} = \frac{1}{p} \sum_{0 < |\ell| \leq p/2} \left( \sum_{y \in I_2^{(j)}} e \left( \frac{-\ell y}{p} \right) \right) \left( \sum_{x \in I_1^{(j)}} e \left( \frac{\ell x}{p} \right) \right)
\ll \sum_{0 < |\ell| \leq p/2} \frac{1}{|\ell|} \left| \sum_{x \in I_1^{(j)}} e \left( \frac{\ell x}{p} \right) \right|.
\]
Applying Cauchy’s inequality and Theorem 2 we deduce that
\[
\sum_{j=1}^{J} |S_{2,j}| \ll \sum_{0<|\ell|\leq p/2} \sum_{j=1}^{J} \sum_{x \in I_{1}^{(j)}} | \sum_{j=1}^{J} e \left( \frac{\ell x}{p} \right) |^{2} \left( \sum_{x \in I_{1}^{(j)}} e \left( \frac{\ell x}{p} \right) \right)^{2} \frac{1}{2} 
\ll J^{1/2} \sum_{0<|\ell|\leq p/2} \frac{1}{|\ell|} \left( \sum_{j=1}^{J} \sum_{x \in I_{1}^{(j)}} e \left( \frac{\ell x}{p} \right) \right)^{2} \frac{1}{2} 
\ll J^{1/2} (\log p) \left( p \log^{2} H \right)^{1/2}.
\]
Under the conditions of Theorem 1 it now follows that (5) dominates this quantity, from which the conclusion of the theorem follows.

References

[1] J.B. Friedlander, H. Iwaniec, Incomplete Kloosterman sums and a divisor problem. *Ann. of Math.* **121** (1985), 319–350.
[2] D.R. Heath-Brown, Arithmetic applications of Kloosterman sums. *Nieuw Arch. Wiskd.* **1** (2000), 380–384.
[3] D.R. Heath-Brown, Burgess’s bounds for character sums. *Submitted*, 2012. [arXiv:1203.5219](http://arxiv.org/abs/1203.5219)
[4] C. Hooley, On the greatest prime factor of a cubic polynomial. *J. reine angew. Math.* **303/304** (1978), 21–50.

School of Mathematics, University of Bristol, Bristol, BS8 1TW, UK
E-mail address: t.d.browning@bristol.ac.uk
E-mail address: alan.haynes@bristol.ac.uk