

New Bounds for Gauss Sums Derived From k -th Powers, and for Heilbronn's Exponential Sum

D.R. Heath-Brown
Magdalen College, Oxford

S. Konyagin
Moscow State University

1 Introduction

This paper is concerned with the Gauss sums

$$G(a) = G_p(a, k) = \sum_{n=1}^p e_p(an^k),$$

and with Heilbronn's sum

$$H(a) = H_p(a) = \sum_{n=1}^p e\left(\frac{an^p}{p^2}\right),$$

where p is prime, $e(x) = \exp(2\pi ix)$, and $e_p(x) = e(x/p)$. In each case we shall assume that $p \nmid a$ unless the contrary is explicitly stated.

Gauss sums arise in investigations into Waring's problem, and other additive problems involving k -th powers. Although they are amongst the simplest complete exponential sums, the question as to their true order of magnitude is far from being resolved. We remark at the outset that if $(k, p-1) = k_0$, then

$$G_p(a, k) = G_p(a, k_0).$$

Thus it suffices to suppose, as indeed we shall, that $k|p-1$.

When $p \nmid a$ the trivial bound for $G(a)$ states that $|G(a)| \leq p$. The next simplest estimate takes the form

$$|G(a)| \leq (k-1)\sqrt{p}. \quad (1)$$

This may be obtained by writing $G(a)$ in terms of the character Gauss sum as

$$G(a) = \sum_{\substack{\chi^k = \chi_0 \\ \chi \neq \chi_0}} \bar{\chi}(a) \tau(\chi). \quad (2)$$

There are $k - 1$ terms here, each of modulus \sqrt{p} . One can also think of the estimate (1) as deriving from Weil's Riemann Hypothesis for curves over finite fields. The formula (2) then gives explicitly the decomposition of $G(a)$ as a linear combination of roots of the corresponding L -function. We should remark that Montgomery, Vaughan and Wooley [5] have given a small improvement on (1), by showing that if $2k \nmid (p - 1)$ then

$$|G(a)| \leq 2^{-1/2}(k^2 - 2k + 2)^{1/2}p^{1/2},$$

for $p > 2$. Moreover they present both numerical and heuristic evidence in support of the conjecture that

$$|G(a)| \leq \min\{(k - 1)p^{1/2}, (1 + \eta)(2kp \log kp)^{1/2}\},$$

where $\eta \rightarrow 0$ as k and p/k tend to infinity. Indeed one expects that this hypothetical upper bound would be best possible.

The estimate (1) is fairly sharp if k is small in comparison with p , but as soon as $k \gg \sqrt{p}$ it becomes worse than the trivial bound. This is a universal problem when one applies Weil's method, (or indeed Deligne's, in the case of multiple exponential sums): For large degree the bound obtained is trivial.

For values of k of intermediate size remarkable progress was made by Shparlinski [6], who established the bound

$$G(a) \ll k^{7/12}p^{2/3}, \tag{3}$$

thereby improving the previous results for $p^{2/5} \leq k \leq p^{4/7}$. Moreover Konyagin and Shparlinski later showed, in unpublished work, that

$$G(a) \ll k^{1/3}p^{19/24}, \tag{4}$$

which improves the three earlier bounds for $p^{1/2} \leq k \leq p^{5/8}$. Both the results (3) and (4) were subsequently found independently by Heath-Brown (unpublished).

Shparlinski reduces the problem of estimating $G(a)$ to that of bounding the number of solutions to a congruence

$$x^k + y^k \equiv n \pmod{p}. \tag{5}$$

This problem is tackled via a theorem of Garcia and Voloch [1]. Heath-Brown's approach is very similar, but the method of Stepanov [7] is used to handle (5). The proof of Garcia and Voloch's estimate has in fact strong parallels with Stepanov's method.

It should also be mentioned that large values of k have been treated by Konyagin [3], who shows that for any $\varepsilon > 0$ there is a positive constant c_ε for which

$$|G(a)| \leq p(1 - \frac{c_\varepsilon}{(\log k)^{1+\varepsilon}})$$

for $k \geq 2$ and

$$p \geq \frac{k \log k}{(\log \log k)^{1-\varepsilon}}.$$

Here we have corrected an unfortunate misprint in the English translation of Konyagin's paper, which led to its being quoted incorrectly in both *Zentralblatt*, (820:11048) and *Math. Reviews*, (96e:11122). Although the improvement over the trivial bound is extremely small, there are important consequences for Waring's problem modulo p , as Konyagin describes.

In the present paper we improve the application of Stepanov's method to bound the number of solutions of (5) for several different values of n simultaneously. This enables us to establish the following improvement of (3).

Theorem 1 *For $p \nmid a$ we have*

$$G(a) \ll \begin{cases} kp^{1/2}, & 1 \leq k \leq p^{1/3}, \\ k^{5/8}p^{5/8}, & p^{1/3} < k \leq p^{1/2}, \\ k^{3/8}p^{3/4}, & p^{1/2} < k \leq p^{2/3}, \\ p, & p^{2/3} < k < p. \end{cases}$$

The trivial bound and the estimate (1) are therefore both superseded for $p^{1/3} \ll k \ll p^{2/3}$.

For many years it was an open problem to show that Heilbronn's sum satisfies $H_p(a) = o(p)$ as $p \rightarrow \infty$. Recently Heath-Brown [2] was able to establish the bound

$$H_p(a) \ll p^{11/12}.$$

The proof used Stepanov's method to bound the number of solutions of the congruence

$$f(x) \equiv u \pmod{p},$$

where

$$f(X) = X + \frac{X^2}{2} + \frac{X^3}{3} + \dots + \frac{X^{p-1}}{p-1},$$

thereby re-discovering a result of Mit'kin [4]. Our new variant of Stepanov's method can be applied here too, yielding the following improved estimate.

Theorem 2 *We have*

$$\sum_{r=1}^p |H_p(a + rp)|^4 \ll p^{7/2}$$

and hence

$$H_p(a) \ll p^{7/8}$$

for $p \nmid a$.

As a corollary, we have a new bound for incomplete Heilbronn sums.

Corollary *If p is a prime and $p \nmid a$ then*

$$\sum_{\substack{M < n \leq M+N \\ p \nmid n}} e\left(\frac{an^p}{p^2}\right) \ll p^{5/8} N^{1/4},$$

uniformly in a , for all M and for all $N \leq p$.

This may be compared with the corresponding result of Heath-Brown [2], in which the bound was $O(p^{11/12})$. The new result is non-trivial for $N \gg p^{5/6}$.

The proofs of our theorems begin with some straightforward manipulation, leading to the following results.

Lemma 1 *Let $h = (p-1)/k$ and set*

$$\mu_h = \{x \in \mathbb{Z}_p : x^h = 1\},$$

$$\mathcal{A}(h) = \{(x_1, x_2, x_3, x_4) \in \mu_h^4 : x_1 + x_2 = x_3 + x_4\}.$$

Then

$$G(a) \ll k^{5/4} (\#\mathcal{A}(h))^{1/4}, \quad (6)$$

and

$$G(a) \ll p^{1/8} k (\#\mathcal{A}(h))^{1/4}. \quad (7)$$

Lemma 2 *Let*

$$f(X) = X + \frac{X^2}{2} + \frac{X^3}{3} + \dots + \frac{X^{p-1}}{p-1} \in \mathbb{Z}_p,$$

and let

$$\mathcal{B} = \{(x_1, x_2) \in \mathbb{Z}_p^2 : f(x_1) = f(x_2)\}.$$

Then

$$\sum_r^p |H_p(a + rp)|^4 \ll p^3 + p^2 \#\mathcal{B}.$$

By applying our new variant of Stepanov's method we shall establish the following bounds for $\#\mathcal{A}(h)$ and $\#\mathcal{B}$, from which Theorems 1 and 2 immediately follow.

Lemma 3 *For any $h < p^{2/3}$ we have $\#\mathcal{A}(h) \ll h^{5/2}$.*

Lemma 4 *We have $\#\mathcal{B} \ll p^{3/2}$.*

The nature of our improvement in the application of Stepanov's method is clearest when one compares Lemma 4 of Heath-Brown [2], with our Lemma 7. If we define

$$\mathcal{F}(u) = \{x \in \mathbb{Z}_p : f(x) = u\}$$

then, in the notation of the current paper, the former result states that

$$\#\mathcal{F}(u) \ll p^{2/3}$$

for any $u \in \mathbb{Z}_p$, while our Lemma 7 shows that

$$\sum_{u \in U} \#\mathcal{F}(u) \ll p^{2/3}(\#U)^{2/3}$$

for any $U \subseteq \mathbb{Z}_p$.

2 Proof of Lemmas 1 and 2

In this section we shall prove Lemmas 1 and 2. We begin by writing

$$G_0(a) = \sum_{n=1}^{p-1} e_p(an^k),$$

so that $G(a) = 1 + G_0(a)$. Then

$$G_0(a) = G_0(am^k) \text{ for } p \nmid m.$$

It follows that

$$(p-1)|G_0(a)|^4 = \sum_{m=1}^{p-1} |G_0(am^k)|^4 \leq k \sum_{n=1}^p |G_0(n)|^4,$$

since each value of n arises either k times or not at all. We therefore see that

$$\begin{aligned} h|G_0(a)|^4 &\leq \sum_{m_1, \dots, m_4=1}^{p-1} \sum_{n=1}^p e_p((m_1^k + m_2^k - m_3^k - m_4^k)n) \\ &= p\#\{(m_1, \dots, m_4) : m_1^k + m_2^k \equiv m_3^k + m_4^k \pmod{p}\} \\ &= pk^4 \# \mathcal{A}(h), \end{aligned}$$

and (6) follows.

To derive (7) we note that

$$(p-1)|G_0(a)|^2 = \sum_{m=1}^{p-1} |G_0(am^k)|^2$$

$$\begin{aligned}
&= \sum_{n_1, n_2=1}^{p-1} \sum_{m=1}^{p-1} e_p(a(n_1^k - n_2^k)m^k) \\
&= \sum_{b=1}^p N(b)G_0(ab),
\end{aligned}$$

where

$$N(b) = \#\{(n_1, n_2) : 1 \leq n_1, n_2 \leq p-1, n_1^k - n_2^k \equiv b \pmod{p}\}.$$

We may now apply Hölder's inequality, whence

$$(p-1)^4 |G_0(a)|^8 \leq \left\{ \sum_{b=1}^p N(b)^2 \right\} \left\{ \sum_{b=1}^p N(b) \right\}^2 \left\{ \sum_{b=1}^p |G_0(ab)|^4 \right\}.$$

As above, the final sum on the right is $pk^4 \#\mathcal{A}(h)$. We may therefore conclude that

$$(p-1)^4 |G_0(a)|^8 \ll pk^4 (\#\mathcal{A}(h)) \left\{ \sum_{b=1}^p N(b)^2 \right\} \left\{ \sum_{b=1}^p N(b) \right\}^2. \quad (8)$$

In order to estimate the terms involving the function $N(b)$, we recall that $h = (p-1)/k$, and observe that the congruence $n^k \equiv s \pmod{p}$ has no solutions unless $s^h \equiv 1 \pmod{p}$, in which case there are exactly k solutions. It therefore follows that $N(b) = k^2 M(b)$, where

$$M(b) = \#\{(x_1, x_2) \in \mu_h^2 : x_1 - x_2 = b\}.$$

We trivially have

$$\sum_{b=1}^p M(b)^2 = \mathcal{A}(h),$$

whence

$$\sum_{b=1}^p N(b)^2 = k^4 \mathcal{A}(h).$$

Moreover it is clear that

$$\sum_{b=1}^p N(b) = (p-1)^2.$$

If we now insert these formulae into (8) we see that the estimate (7) follows immediately.

The proof of Lemma 2 is similar to that of (6). We write

$$H_0(a) = \sum_{n=1}^{p-1} e\left(\frac{an^p}{p^2}\right),$$

so that $H(a) = 1 + H_0(a)$. Then

$$H_0(a) = H_0(am^p) \text{ for } p \nmid m.$$

It follows that

$$(p-1) \sum_{r=1}^p |H_0(a+rp)|^4 = \sum_{r=1}^p \sum_{m=1}^{p-1} |H_0((a+rp)m^p)|^4 \leq \sum_{n=1}^{p^2} |H_0(n)|^4,$$

since each value of n arises at most once. (Indeed each value with $p \nmid n$ arises exactly once.) We therefore see that

$$\begin{aligned} (p-1) \sum_{r=1}^p |H_0(a+rp)|^4 &\leq \sum_{m_1, \dots, m_4=1}^{p-1} \sum_{n=1}^{p^2} e_{p^2}((m_1^p + m_2^p - m_3^p - m_4^p)n) \\ &= p^2 \#\{1 \leq m_1, \dots, m_4 \leq p-1 : m_1^p + m_2^p \equiv m_3^p + m_4^p \pmod{p^2}\}. \end{aligned}$$

Here we must have $m_1 + m_2 \equiv m_3 + m_4 \pmod{p}$. Thus, if we write

$$m_1 - m_3 \equiv b \pmod{p}$$

we also have $m_4 - m_2 \equiv b \pmod{p}$. The case $p|b$ now contributes $(p-1)^2$ solutions of the congruence. When $p \nmid b$ we write $m_1 \equiv v_1 b \pmod{p}$, so that $m_3 \equiv (v_1 - 1)b \pmod{p}$. Thus

$$m_1^p - m_3^p \equiv (v_1^p - (v_1 - 1)^p)b^p \pmod{p^2}.$$

In the same way we find that

$$m_4^p - m_2^p \equiv (v_2^p - (v_2 - 1)^p)b^p \pmod{p^2},$$

where $m_4 \equiv v_2 b \pmod{p}$.

The congruence $m_1^p + m_2^p \equiv m_3^p + m_4^p \pmod{p^2}$ now becomes

$$(v_1^p - (v_1 - 1)^p)b^p \equiv (v_2^p - (v_2 - 1)^p)b^p \pmod{p^2}.$$

There are $p-1$ choices for b , and for each such value we will have

$$v_1^p - (v_1 - 1)^p \equiv v_2^p - (v_2 - 1)^p \pmod{p^2}.$$

Since

$$v^p - (v-1)^p = \sum_{l=1}^p (-1)^{l-1} v^{p-l} \binom{p}{l} \equiv 1 - pf(v) \pmod{p^2},$$

it now follows that

$$\begin{aligned} &\#\{1 \leq m_1, \dots, m_4 \leq p-1 : m_1^p + m_2^p \equiv m_3^p + m_4^p \pmod{p^2}\} \\ &\leq (p-1)^2 + (p-1) \#\{1 \leq v_1, v_2 \leq p-1 : f(v_1) \equiv f(v_2) \pmod{p}\}, \end{aligned}$$

whence

$$(p-1) \sum_{r=1}^p |H_0(a+rp)|^4 \leq p^2 \{(p-1)^2 + (p-1) \#\mathcal{B}\}$$

which suffices for Lemma 2.

3 Stepanov's Method

We shall begin by considering $\#\mathcal{A}(h)$. For each $u \in \mathbb{Z}_p$ we write

$$\mathcal{C}(u) = \{x \in \mu_h : x - u \in \mu_h\},$$

so that $\#\mathcal{C}(0) = h$ and

$$\begin{aligned} \#\mathcal{A}(h) &= \sum_{u \in \mathbb{Z}_p} (\#\mathcal{C}(u))^2 \\ &= h^2 + \sum_{u \neq 0} (\#\mathcal{C}(u))^2 \\ &= h^2 + h \sum_u^* (\#\mathcal{C}(u))^2 \end{aligned} \tag{9}$$

where Σ^* indicates that u runs over distinct coset representatives of μ_h in \mathbb{Z}_p^\times .

In the same way we have

$$\begin{aligned} \{\#\mu_h\}^2 &= \sum_{u \in \mathbb{Z}_p} \#\mathcal{C}(u) \\ &= h + \sum_{u \neq 0} \#\mathcal{C}(u) \\ &= h + h \sum_u^* \#\mathcal{C}(u), \end{aligned}$$

whence

$$\sum_u^* \#\mathcal{C}(u) = h - 1. \tag{10}$$

We now take an arbitrary set U of elements u from distinct cosets of \mathbb{Z}_p^\times , and write

$$\mathcal{D}(u) = u^{-1}\mathcal{C}(u) = \{y \in \mathbb{Z}_p : uy \in \mu_h, uy - u \in \mu_h\},$$

and

$$\mathcal{E} = \bigcup_{u \in U} \mathcal{D}(u).$$

Thus $\#\mathcal{D}(u) = \#\mathcal{C}(u)$, and since the sets $\mathcal{D}(u)$ are disjoint we deduce that

$$\#\mathcal{E} = \sum_{u \in U} \#\mathcal{C}(u).$$

Our aim is to prove the following bound for $\#\mathcal{E}$.

Lemma 5 *Let $\#U = T \geq 1$. Then*

$$\#\mathcal{E} \ll (hT)^{2/3}$$

providing that $h^4T < p^3$.

We begin our application of Stepanov's method by taking a polynomial $\Phi(X, Y, Z) \in \mathbb{Z}_p[X, Y, Z]$, for which

$$\deg_X \Phi < A, \deg_Y \Phi < B, \deg_Z \Phi < B,$$

and arranging that the polynomial

$$\Psi(X) = \Phi(X, X^h, (X-1)^h)$$

has a zero of order at least D , say, at each point $x \in \mathcal{E}$. We will therefore be able to conclude that $D\#\mathcal{E} \leq \deg \Psi(X)$, providing that Ψ does not vanish identically. We note that

$$\deg \Psi \leq (\deg_X \Phi) + h(\deg_Y \Phi) + h(\deg_Z \Phi) < A + 2hB,$$

whence

$$D\#\mathcal{E} \ll A + hB, \tag{11}$$

providing that Ψ does not vanish.

In order for Ψ to have a zero of multiplicity at least D at a point x we need

$$\left(\frac{d}{dX} \right)^n \Psi(X) \Big|_{X=x} = 0 \quad \text{for } n < D.$$

Since $x \neq 0, 1$ for $x \in \mathcal{E}$, this will be equivalent to

$$\{X(X-1)\}^n \left(\frac{d}{dX} \right)^n \Psi(X) \Big|_{X=x} = 0. \tag{12}$$

We now observe that

$$X^m \left(\frac{d}{dX} \right)^m X^a = \frac{a!}{(a-m)!} X^a,$$

$$X^m \frac{d^m}{dX^m} X^{hb} = \frac{(hb)!}{(hb-m)!} X^{hb},$$

and

$$(X-1)^m \left(\frac{d}{dX} \right)^m (X-1)^{hc} = \frac{(hc)!}{(hc-m)!} (X-1)^{hc}.$$

It follows that

$$\{X(X-1)\}^n \left(\frac{d}{dX} \right)^n X^a X^{hb} (X-1)^{hc} = P_{n,a,b,c}(X) X^{hb} (X-1)^{hc}$$

where $P_{n,a,b,c}(X)$ either vanishes or is a polynomial of degree $n+a$. We therefore deduce that

$$\{X(X-1)\}^n \left(\frac{d}{dX} \right)^n X^a X^{hb} (X-1)^{hc} \Big|_{X=x} = u^{-hb-hc} P_{n,a,b,c}(x)$$

for any $x \in \mathcal{D}(u)$. Here we use the fact that $x^h = (x-1)^h = u^{-h}$ for such x .

We now write

$$\Phi(X, Y, Z) = \sum_{a,b,c} \lambda_{a,b,c} X^a Y^b Z^c$$

and

$$P_{n,u}(X) = \sum_{a,b,c} \lambda_{a,b,c} u^{-hb-hc} P_{n,a,b,c}(X),$$

so that $\deg P_{n,u}(X) < A+n$ and

$$\{X(X-1)\}^n \left(\frac{d}{dX} \right)^n \Phi(X, X^h, (X-1)^h) \Big|_{X=x} = P_{n,u}(x)$$

for any x in $\mathcal{D}(u)$. We shall arrange, by appropriate choice of the coefficients $\lambda_{a,b,c}$, that $P_{n,u}(X)$ vanishes identically for $n < D$, for all $u \in U$. This will ensure that (12) holds for $x \in \mathcal{E}$. Each of the polynomials $P_{n,u}(X)$ has at most $A+n \leq A+D$ coefficients, which are linear forms in the original $\lambda_{a,b,c}$. Thus if

$$D(A+D)T < AB^2, \quad (13)$$

there will be a set of coefficients $\lambda_{a,b,c}$, not all zero, for which the polynomials $P_{n,u}(X)$ vanish for all $n < D$ and all $u \in U$.

We must now consider whether $\Phi(X, X^h, (X-1)^h)$ can vanish if $\Phi(X, Y, Z)$ does not. We shall write

$$\Phi(X, Y, Z) = \sum_c \Phi_c(X, Y) Z^c,$$

and take c_0 to be the smallest value of c for which $\Phi_c(X, Y)$ is not identically zero. It follows that

$$\Phi(X, X^h, (X-1)^h) = (X-1)^{hc_0} \sum_{c_0 \leq c < B} \Phi_c(X, X^h) (X-1)^{h(c-c_0)},$$

so that if $\Phi(X, X^h, (X-1)^h)$ is identically zero we must have

$$\Phi_{c_0}(X, X^h) \equiv 0 \pmod{(X-1)^h}. \quad (14)$$

At the end of this section we shall establish the following result.

Lemma 6 *Let $P(X) \in \mathbb{Z}_p[X]$ be a sum of $N \geq 1$ distinct monomials. Suppose further that $\deg(P) < p$. Then $(X-1)^N$ cannot divide $P(X)$.*

Lemma 6 shows that (14) is impossible, providing that

$$AB \leq h \quad \text{and} \quad A + hB < p. \quad (15)$$

We now choose our parameters A and B by taking

$$A = \left\lfloor \frac{1}{2} h^{2/3} T^{-1/3} \right\rfloor \quad \text{and} \quad B = \left\lfloor \frac{1}{2} h^{1/3} T^{1/3} \right\rfloor.$$

These will produce positive integers satisfying (15), providing that $h^2 \geq 8T$ and $h^4 T < p^3$. Moreover there will then be an integer T for which (13) holds, in the range $h^{2/3} T^{-1/3} \ll D \ll h^{2/3} T^{-1/3}$. The estimate (11) therefore produces

$$\#\mathcal{E} \ll hB/D \ll (hT)^{2/3}$$

as required. Of course, if $T \gg h^2$, then the bound (10) yields

$$\#\mathcal{E} \ll h \ll (hT)^{2/3},$$

and Lemma 5 is trivial.

We turn now to the argument required for Lemma 4. This will be an adaption of that given by Heath-Brown [2], along the lines used above. Thus we write

$$\mathcal{F}(u) = \{x \in \mathbb{Z}_p : f(x) = u\},$$

so that

$$\#\mathcal{B} = \sum_{u \in \mathbb{Z}_p} (\#\mathcal{F}(u))^2 \quad (16)$$

and

$$\sum_{u \in \mathbb{Z}_p} \#\mathcal{F}(u) = p. \quad (17)$$

Moreover we set

$$\mathcal{G} = \bigcup_{u \in U} \mathcal{F}(u),$$

where U is an arbitrary set of T elements $u \in \mathbb{Z}_p$. In analogy to Lemma 5 we aim to prove the following bound.

Lemma 7 *Let $\#U = T \geq 1$. Then*

$$\#\mathcal{G} \ll (pT)^{2/3}.$$

We begin by choosing $\Phi(X, Y, Z) \in \mathbb{Z}_p[X, Y, Z]$, with

$$\deg_X \Phi < A, \quad \deg_Y \Phi < B, \quad \deg_Z \Phi < C.$$

We shall arrange that the polynomial

$$\Psi(X) = \Phi(X, f(X), X^p)$$

has a zero of order at least D , say, at each point $x \in \mathcal{G}$. We will then be able to deduce that $D\#\mathcal{G} \leq \deg \Psi(X)$, providing that Ψ does not vanish identically. We note that

$$\deg \Psi \leq (\deg_X \Phi) + (p-1)(\deg_Y \Phi) + p(\deg_Z \Phi) < A + p(B+C),$$

whence

$$D\#\mathcal{G} \ll A + p(B+C), \quad (18)$$

providing that Ψ does not vanish.

Following the argument of [2;§§3& 4] this can be achieved by making certain polynomials $P_{n,u}(X)$ of degree less than $A + 2D + C$ vanish identically, for all $n < D$ and each $u \in U$. The coefficients of these polynomials are linear forms in the coefficients of the original function Φ , so that it suffices to have

$$D(A + 2D + C)T < ABC.$$

Moreover Lemma 3 of [2] shows that Ψ will not vanish identically, providing that

$$AB \leq p.$$

We therefore choose

$$A = [p^{2/3}T^{-1/3}], \quad B = C = [p^{1/3}T^{1/3}],$$

which are clearly admissible, since $T = \#U \leq p$. Moreover we may take

$$D = [p^{2/3}T^{-1/3}/16],$$

which is also satisfactory, if p is large enough. It then follows from (18) that

$$\#\mathcal{G} \ll p^{2/3}T^{2/3}$$

as required.

It remains to establish Lemma 6. This will be achieved by induction on N . The case $N = 1$ is trivial. Now suppose that $N > 1$, and let

$$P(X) = \sum_l c_l X^l,$$

where l runs over N distinct values. Then

$$XP'(X) - l_0 P(X) = \sum_l c_l (l - l_0) X^l.$$

Now, on choosing l_0 to be, say, the degree of the highest order term in $P(X)$, we produce a polynomial containing exactly $N-1$ terms. We then see that $(X-1)^N$ cannot divide $P(X)$, for otherwise $(X-1)^{N-1}$ would divide $XP'(X) - l_0 P(X)$, contrary to our induction hypothesis. This completes the proof of Lemma 6.

4 Deduction of Lemmas 3 and 4

We shall now use Lemma 5, in conjunction with (9) and (10), to bound $\#\mathcal{A}(h)$. Since we are assuming that $h \leq p^{2/3}$ it is automatic that

$$h^4 T \leq h^4 k = h^3(p-1) < p^3.$$

We number the coset representatives u as u_i , $1 \leq i \leq k$, in such a way that

$$\#\mathcal{C}(u_1) \geq \#\mathcal{C}(u_2) \geq \dots$$

If we now take U to be the set of u_i for $i \leq T$ then Lemma 5 shows that

$$T\#\mathcal{C}(u_T) \leq \#\mathcal{E} \ll (hT)^{2/3}$$

for any T . Hence

$$\sum_{N/2 < T \leq N} (\#\mathcal{C}(u_T))^2 \ll N(h^{2/3}N^{-1/3})^2 = h^{4/3}N^{1/3}.$$

Alternatively we may use (10), which yields

$$\sum_{N/2 < T \leq N} (\#\mathcal{C}(u_T))^2 \ll h^{2/3}N^{-1/3}(h-1) \ll h^{5/3}N^{-1/3}.$$

If we now sum over $N = 1, 2, 4, 8, \dots$, using the first bound for $N \leq h^{1/2}$ and the second estimate otherwise, we find that

$$\sum_u^* (\#\mathcal{C}(u))^2 \ll h^{3/2},$$

so that Lemma 3 follows from (9).

The deduction of Lemma 4 from (16), (17) and Lemma 7 is, of course, completely analogous.

5 The Corollary to Theorem 2

As in Heath-Brown [2], the standard procedure for completing an incomplete exponential sum yields

$$\begin{aligned} \sum_{\substack{M < n \leq M+N \\ p \nmid n}} e\left(\frac{an^p}{p^2}\right) &= p^{-1} \sum_{r=1}^p \sum_{s=1}^p e\left(\frac{as^p}{p^2}\right) \sum_{M < n \leq M+N} e\left(\frac{r(s-n)}{p}\right) \\ &\ll p^{-1} \sum_{r=1}^p \min\left\{N, \frac{1}{\|r/p\|}\right\} \left| \sum_{s=1}^p e\left(\frac{as^p}{p^2}\right) e\left(\frac{rs}{p}\right) \right|, \end{aligned}$$

on using the estimates

$$\sum_{M < n \leq M+N} e\left(\frac{-rn}{p}\right) \ll \begin{cases} N, & \text{any } r, \\ \frac{1}{\|r/p\|}, & p \nmid r. \end{cases}$$

However, since $s \equiv s^p \pmod{p}$, we have

$$e\left(\frac{as^p}{p^2}\right)e\left(\frac{rs}{p}\right) = e\left(\frac{(a+rp)s^p}{p^2}\right),$$

so that

$$\sum_{s=1}^p e\left(\frac{as^p}{p^2}\right)e\left(\frac{rs}{p}\right) = H(a+rp),$$

and hence

$$\sum_{\substack{M < n \leq M+N \\ p \nmid n}} e\left(\frac{an^p}{p^2}\right) \ll p^{-1} \sum_{r=1}^p \min\left\{N, \frac{1}{\|r/p\|}\right\} |H(a+rp)|.$$

We may now apply Hölder's inequality, whence

$$\begin{aligned} & \sum_{\substack{M < n \leq M+N \\ p \nmid n}} e\left(\frac{an^p}{p^2}\right) \\ & \ll p^{-1} \left\{ \sum_{r=1}^p \min\left\{N, \frac{1}{\|r/p\|}\right\}^{4/3} \right\}^{3/4} \left\{ \sum_{r=1}^p |H(a+rp)|^4 \right\}^{1/4} \\ & \ll p^{-1/8} \left\{ \sum_{r=1}^p \min\left\{N, \frac{1}{\|r/p\|}\right\}^{4/3} \right\}^{3/4}, \end{aligned}$$

by Theorem 2. Since $N \leq p$ and

$$\sum_{r=1}^p \min\left\{N, \frac{1}{\|r/p\|}\right\}^{4/3} \ll pN^{1/3},$$

we deduce that

$$\sum_{\substack{M < n \leq M+N \\ p \nmid n}} e\left(\frac{an^p}{p^2}\right) \ll p^{5/8} N^{1/4},$$

as claimed.

6 Acknowledgement

The second author was supported by Grants 96-01-00378 from the Russian Foundation for Basic Research and 96-15-96072 from the Programme of Development of Scientific Schools.

References

- [1] A. Garcia and J. F. Voloch, Fermat Curves Over Finite Fields, *J. Number Theory*, 30 (1988), 345-356.
- [2] D.R. Heath-Brown, An estimate for Heilbronn's exponential sum, *Analytic number theory: Proceedings of a conference in honor of Heini Halberstam*, (Birkhäuser, Boston, 1996), 451-463.
- [3] S.V. Konyagin, On estimates of Gaussian sums and Waring's problem for a prime modulus, *Proc. Steklov Inst. Math.*, 198 (1994), 105-117.
- [4] D.A. Mit'kin, An estimate for the number of roots of some comparisons by the Stepanov method, *Mat. Zametki*, 51 (1992), 52-58, 157. (Translated as *Math. Notes*, 51 (1992), 565-570.)
- [5] H.L. Montgomery, R.C. Vaughan, and T.D. Wooley, Some remarks on Gauss sums associated with k th powers, *Math. Proc. Camb. Phil. Soc.*, 118 (1995), 21-33.
- [6] I. E. Shparlinski, On Bounds of Gaussian Sums, *Mat. Zametki*, 50 (1991), 122-130.
- [7] S.A. Stepanov, The number of points of a hyperelliptic curve over a prime field, *Izv. Akad. Nauk SSSR Ser. Mat.*, 33 (1969), 1171-1181.