

HEILBRONN'S CONJECTURE ON WARING'S NUMBER (MOD P)

JAME ARTHUR CIPRA, TODD COCHRANE, AND CHRISTOPHER PINNER

ABSTRACT. Let p be a prime $k|p-1$, $t = (p-1)/k$ and $\gamma(k, p)$ be the minimal value of s such that every number is a sum of s k -th powers (mod p). We prove Heilbronn's conjecture that $\gamma(k, p) \ll k^{1/2}$ for $t > 2$. More generally we show that for any positive integer q , $\gamma(k, p) \leq C(q)k^{1/q}$ for $\phi(t) \geq q$. A comparable lower bound is also given. We also establish exact values for $\gamma(k, p)$ when $\phi(t) = 2$. For instance, when $t = 3$, $\gamma(k, p) = a + b - 1$ where $a > b > 0$ are the unique integers with $a^2 + b^2 + ab = p$, and when $t = 4$, $\gamma(k, p) = a - 1$ where $a > b > 0$ are the unique integers with $a^2 + b^2 = p$.

1. INTRODUCTION

Let p be a prime. The smallest s such that

$$(1) \quad x_1^k + x_2^k + \cdots + x_s^k \equiv N \pmod{p}$$

has a solution for all integers N is called Waring's number (mod p), denoted $\gamma(k, p)$. If $d = (k, p-1)$ then clearly $\gamma(d, p) = \gamma(k, p)$. Hence, we will assume $k|p-1$, and let $t = \frac{p-1}{k}$. It is easy to see that $\gamma(p-1, p) = p-1$ and $\gamma(\frac{1}{2}(p-1), p) = \frac{1}{2}(p-1)$, so we will assume $t > 2$. For such t the k -th powers (mod p) are scattered and so one expects much better bounds for $\gamma(k, p)$. For example when $t = 3$ the k -th powers are just the cube roots of 1 (mod p) and $\gamma(k, p)$ is the smallest s such that every integer is a sum of s cube roots of 1 (mod p). From Theorem 2 we obtain for $t = 3, 4$ or 6 that

$$(2) \quad \sqrt{2k} - 1 \leq \gamma(k, p) \leq 2\sqrt{k}.$$

Indeed, we give the exact value of $\gamma(k, p)$ in these three cases.

Heilbronn [14] made the following conjectures:

I: For any $\varepsilon > 0$, $\gamma(k, p) \ll_{\varepsilon} k^{\varepsilon}$ for $t > t_{\varepsilon}$, and

II: For $t > 2$, $\gamma(k, p) \ll k^{1/2}$.

In view of the inequality in (2) the exponent $\frac{1}{2}$ in the second Heilbronn conjecture is best possible for arbitrary $t > 2$, although as we shall see in Theorem 1, one can do better when $\phi(t) > 2$, in particular $\gamma(k, p) \ll k^{\frac{1}{4}}$. Konyagin [15] proved the first Heilbronn conjecture. His work was refined in [6]. In this paper we prove the second Heilbronn conjecture.

2. HISTORICAL BACKGROUND

Hardy and Littlewood [13] established the uniform bound $\gamma(k, p) \leq k$ for all k, p, t . Henceforth we assume $t > 2$ and $k > 1$. Under this assumption their bound

was refined by S. Chowla, Mann and Straus [5] to

$$(3) \quad \gamma(k, p) \leq [k/2] + 1.$$

I. Chowla [4] proved $\gamma(k, p) \ll k^{0.8771}$; Dodson [8], $\gamma(k, p) \leq k^{7/8}$, for k sufficiently large; Tietäväinen [19], $\gamma(k, p) \ll_{\epsilon} k^{\frac{3}{5}+\epsilon}$; Dodson and Tietäväinen [9],

$$(4) \quad \gamma(k, p) < 68(\log k)^2 k^{1/2}.$$

Bovey [3] also obtained $\gamma(k, p) \ll_{\epsilon} k^{\frac{1}{2}+\epsilon}$. The latter bounds fall just short of the second Heilbronn conjecture.

From Weil's estimate [20] on the number of solutions of (1) one obtains a very small value for $\gamma(k, p)$ for p sufficiently large relative to k :

$$(5) \quad \gamma(k, p) \leq s \quad \text{for } p > k^{\frac{2s}{s-1}}.$$

In particular $\gamma(k, p) \leq 2$ for $p > k^4$, $\gamma(k, p) \leq 3$ for $p > k^3$ and $\gamma(k, p) \leq 3 \log_2(k)$ for $p > 2k^2$. Dodson obtained a similar bound

$$(6) \quad \gamma(k, p) \leq [32 \ln k] + 1 \quad \text{for } p > k^2.$$

It is well known that a uniform bound on the Gauss sum of the type

$$(7) \quad \left| \sum_{x=1}^p e_p(ax^k) \right| \leq \Phi$$

leads immediately to the estimate

$$(8) \quad \gamma(k, p) \leq s \quad \text{for } p > \Phi^{\frac{s}{s-1}}.$$

From the bounds of Heath-Brown and Konyagin [12], $\Phi \ll k^{\frac{5}{8}} p^{\frac{5}{8}}$, $\Phi \ll k^{\frac{3}{8}} p^{\frac{3}{4}}$, one obtains respectfully,

$$(9) \quad \gamma(k, p) \leq s \quad \text{for } p \gg k^{\frac{5s}{3s-8}}, \quad p \gg k^{\frac{3s}{2s-8}}.$$

Results of Bourgain and Konyagin announced in [2] (see Bourgain, Glibichuk and Konyagin [1] for more details) readily yield

$$(10) \quad \gamma(k, p) \leq c(\epsilon) \quad \text{for } p \gg k^{1+\epsilon},$$

for any $\epsilon > 0$. Further estimates can be gleaned from Konyagin's [16] refinement of [12]. It was Konyagin's nontrivial estimate of Φ for large k that lead to the estimate [15, Theorem 2]

$$(11) \quad \gamma(k, p) \ll_{\epsilon} (\ln k)^{2+\epsilon} \quad \text{for } p \geq \frac{k \ln k}{(\ln(\ln k + 1))^{1-\epsilon}},$$

and the proof of the first Heilbronn conjecture.

Finally we note the estimate of Garcia and Voloch [11]

$$(12) \quad \gamma(k, p) \leq 170 \frac{k^{7/3}}{(p-1)^{4/3}} \ln p, \quad \text{for } p \leq k^{7/4} + 1.$$

3. PROOF OF THE SECOND HEILBRONN CONJECTURE

We shall prove

Theorem 1. *Let q be a positive integer. If $\phi(t) \geq q$ then $\gamma(k, p) \leq C(q) k^{1/q}$ for some constant $C(q)$.*

The second Heilbronn conjecture is just the case $q = 2$. The first Heilbronn conjecture is obtained by taking $q > 1/\epsilon$. One also recovers from the theorem (or more specifically Lemma 3) the bound of Heilbronn [14, Theorem 8],

$$\gamma(k, p) \leq c_t k^{1/\phi(t)},$$

for some constant c_t . In section 5 we establish the comparable lower bound,

$$(13) \quad \gamma(k, p) \gg \frac{1}{\sqrt{\log t}} k^{1/\phi(t)}.$$

We deduce the theorem from the following Gauss sum estimate of Cochrane, Pinner and Rosenhouse [6, Theorem 1.1].

Lemma 1. *For $p \geq p_0$*

$$(14) \quad \left| \sum_{x=1}^p e_p(ax^k) \right| \leq p \left(1 - \frac{1}{p^{2/\phi(t)} \log p (\log \log p)^5} \right).$$

One immediately deduces from (8),

Lemma 2. *If $p \geq p_0$ then $\gamma(k, p) \leq p^{2/\phi(t)} (\log p)^2 (\log \log p)^5$.*

We also need the following result of Bovey [3, Theorem 1],

Lemma 3. *For any positive integer q , there exist numbers $c(q)$ and $t_0(q)$ such that*
i) $\gamma(k, p) \leq c(q) \phi(t) k^{1/q}$ for $t > t_0(q)$
ii) $\gamma(k, p) \leq c(q) k^{1/\phi(t)}$ for $t \leq t_0(q)$

A bound of this general type, namely $\gamma(k, p) \leq c(q) t p^{2/q} \log p$ for $\phi(t) \geq q$, also follows from Theorem 4.2 of [17]. We also note that the Bourgain and Konyagin bound (10) can be used in place of Lemma 2 to deal with the large values of t (say $t > p^{1/4q}$, using Lemma 3 if $t_0(2q) < t \leq p^{1/4q}$ or $t \leq t_0(2q)$).

We turn now to the proof of the theorem. Suppose $\phi(t) \geq q$. Dodson's result (6) lets us restrict our attention to $k^2 \geq p$. For $\phi(t) \geq 2(2q+1)$ we use Lemma 2:

$$\gamma(k, p) \leq p^{\frac{1}{2q+1}} (\log p)^2 (\log \log p)^5 \leq p^{\frac{1}{2q}} \leq k^{1/q}$$

for $p \geq c_1(q)$, with trivially $\gamma(k, p) \leq p-1 < c_1(q)$ otherwise. In the remaining cases, $q \leq \phi(t) < 2(2q+1)$, Lemma 3 immediately gives

$$\gamma(k, p) \leq c(q) 2(2q+1) k^{1/q}.$$

Taken together we see that $\gamma(k, p) \leq C(q) k^{1/q}$ for some constant $C(q)$.

4. THE CASE $\phi(t) = 2$.

Let $\delta(k, p)$ be the minimal value of s so that every integer N can be written as a plus-minus sum of s k -th powers (mod p), that is, $\pm x_1^k \pm x_2^k \pm \dots \pm x_s^k \equiv N \pmod{p}$ is solvable. In the following theorem we give the exact value of $\delta(k, p)$ and $\gamma(k, p)$ for the three values of t with $\phi(t) = 2$, namely, $t = 3, 4, 6$.

Theorem 2. *a) Let $t = 3$ or 6 and a, b be the unique positive integers with $a > b$ and $a^2 + b^2 + ab = p$. Then $\delta(k, p) = \lfloor \frac{2}{3}a + \frac{1}{3}b \rfloor$. If $t = 3$, $\gamma(k, p) = a + b - 1$. If $t = 6$, $\gamma(k, p) = \delta(k, p)$.*

b) Let $t = 4$ and a, b be the unique positive integers with $a > b$ and $a^2 + b^2 = p$. Then $\gamma(k, p) = \delta(k, p) = a - 1$.

From the theorem one readily obtains the bounds

$$\begin{aligned} \sqrt{3k} - \frac{1}{2} &< \gamma(k, p) < 2\sqrt{k}, & \text{when } t = 3, \\ \sqrt{2k} - 1 &\leq \gamma(k, p) \leq 2\sqrt{k} - 1, & \text{when } t = 4, \\ \sqrt{2k} - \frac{1}{2} &< \gamma(k, p) < \frac{2}{3}\sqrt{6k}, & \text{when } t = 6, \end{aligned}$$

and (2) follows immediately. These bounds sharpen the lower bound of Dodson and Tietäväinen [9, Theorem 2], for $t = 3$, $\gamma(k, p) \geq \frac{1}{2}(\sqrt{3k} - 1)$, and the upper bound of Bovey, [3, Lemma 5]. The method we use here is a refinement of ideas from Bovey, [3].

Proof. We start with the easy case $t = 4$. In this case $p \equiv 1 \pmod{4}$, p has a unique representation of the form $p = a^2 + b^2$ with $a > b > 0$, and -1 is a k -th power, so that $\delta(k, p) = \gamma(k, p)$. Let $R \equiv ab \pmod{p}$, so that $R^2 \equiv -1 \pmod{p}$. The set of k -th powers \pmod{p} is just the set $\{\pm 1, \pm R\}$, and so representing a number as a minimal sum of k -th powers is equivalent to representing it in the form $x - Ry$ with $|x| + |y|$ minimal. Let \mathcal{L} be the lattice of points in \mathbb{Z}^2 satisfying the linear congruence

$$(15) \quad x - Ry \equiv 0 \pmod{p}.$$

Then \mathcal{L} is a lattice of volume p with basis (a, b) , $(-b, a)$. Let \mathcal{P} be the parallelogram centered at the origin

$$\mathcal{P} = \left\{ x(a, b) + y(-b, a) : -\frac{1}{2} < x \leq \frac{1}{2}, -\frac{1}{2} < y \leq \frac{1}{2} \right\}.$$

Then \mathcal{P} contains p distinct integer points and the mapping $\eta : \mathcal{P} \cap \mathbb{Z}^2 \rightarrow \mathbb{Z}/(p)$ given by $\eta(x, y) = x - Ry$ is one-to-one and onto. Let f be the mapping $f(x, y) = |x| + |y|$. Then f restricted to \mathcal{P} takes on its maximum value at the corner points $\pm(\frac{a-b}{2}, \frac{a+b}{2}), \pm(\frac{a+b}{2}, \frac{b-a}{2})$. Since a, b have opposite parity, f restricted to the integer points in \mathcal{P} takes on its maximum value at $\pm(\frac{a-b-1}{2}, \frac{a+b-1}{2}), \pm(\frac{a+b-1}{2}, \frac{b-a+1}{2})$ where $f(x, y) = a - 1$ and η takes on the values $\pm 2(1 \pm R) \pmod{p}$. Thus, given any value N there exist integers x, y with $x - Ry \equiv N \pmod{p}$ and $|x| + |y| \leq a - 1$ and so $\delta(k, p) \leq a - 1$. Moreover, it is not hard to see that the values $\pm 2(1 \pm R)$ cannot be represented by any fewer than $a - 1$ k -th powers.

We treat the cases $t = 3$, $t = 6$ simultaneously. The only difference is that when $t = 6$, -1 is a k -th power and so $\delta(k, p) = \gamma(k, p)$. In both these cases $p \equiv 1 \pmod{3}$. The form $x^2 + y^2 + xy$ is the unique reduced positive definite form of discriminant -3 and thus since -3 is a square \pmod{p} , p has a unique representation of the form $p = a^2 + b^2 + ab$ with $a > b > 0$. Let $R \equiv ab \pmod{p}$, a primitive cube root of $1 \pmod{p}$, so that $1 + R + R^2 \equiv 0 \pmod{p}$. In this case the lattice \mathcal{L} given by $x + yR \equiv 0 \pmod{p}$ will have basis $(a, -b)$, $(b, a + b)$. Thus every integer N can be represented in the form $u + Rv \equiv N \pmod{p}$ with integers,

$(u, v) = c_1(a, -b) + c_2(b, a + b) = (c_1a + c_2b, c_2(a + b) - c_1b)$ for some $|c_i| \leq \frac{1}{2}$, satisfying

$$|u| \leq \frac{1}{2}(a + b), \quad |v| \leq \frac{1}{2}a + b, \quad |u| + |v| \leq a + \frac{1}{2}b,$$

the latter inequality following from the fact that $|u| + |v|$ attains a maximum value when the $c_i = \pm \frac{1}{2}$.

Now, the set of k -th powers is $\{1, R, R^2\}$ when $t = 3$ and $\{\pm 1, \pm R, \pm R^2\}$ when $t = 6$ and so representing N as a sum of k -th powers amounts to solving the congruence

$$(16) \quad x + yR + zR^2 \equiv N \pmod{p}.$$

Clearly (x, y, z) satisfies this congruence iff $(x - z - u, y - z - v)$ is in the lattice \mathcal{L} or equivalently

$$(17) \quad x = u + z + \lambda b + \mu a, \quad y = v + z + \lambda(a + b) - \mu b$$

for some integers λ, μ .

We begin by showing the existence of such integers x, y, z with $|x| + |y| + |z| \leq \frac{2}{3}a + \frac{1}{3}b$. Clearly we may assume that $u \geq 0$ (else work with $-x, -y, -z$) and that $u + |v| > \frac{2}{3}a + \frac{1}{3}b$ (else we are done). If $0 \leq v \leq \frac{1}{2}(a + b)$ then $\mu = \lambda = 0$, $z = -\min\{u, v\}$ in (17) gives

$$|x| + |y| + |z| = (u - |z|) + (v - |z|) + |z| = \max\{u, v\} \leq \frac{1}{2}(a + b),$$

while if $v > \frac{1}{2}(a + b)$ (and hence $c_2 > 0, c_1 < 0$ and $u \leq \frac{1}{2}b$) then $\mu = 0, \lambda = -1$, $z = \min\{b - u, a + b - v\}$ in (17) gives

$$|x| + |y| + |z| = (b - u - z) + (a + b - v - z) + z = \max\{b - u, a + b - v\} < \frac{1}{2}(a + b).$$

If $v < 0$ then $\mu = -1, \lambda = 0$ in (17) produces

$$|x| + |y| + |z| = |a - u - z| + |b + z - |v|| + |z|$$

and if $|v| \leq b$ taking $z = 0$ yields

$$|x| + |y| + |z| = (a - u) + b - |v| < \frac{1}{3}a + \frac{2}{3}b,$$

while if $|v| > b$ and $u \geq \frac{1}{3}(a - b)$ then $z = \min\{a - u, |v| - b\}$ has

$$\begin{aligned} |x| + |y| + |z| &= (a - u - z) + (|v| - b - z) + z \\ &= \max\{a - u, |v| - b\} \leq \max\left\{\frac{2}{3}a + \frac{1}{3}b, \frac{1}{2}a\right\} = \frac{2}{3}a + \frac{1}{3}b. \end{aligned}$$

In the remaining case $v < 0, u < \frac{1}{3}(a - b)$, we have $|v| > \frac{2}{3}a + \frac{1}{3}b - u > \frac{1}{3}a + \frac{2}{3}b$, and (17) with $\mu = 0, \lambda = 1, z = -\min\{u + b, a + b - |v|\}$ yields

$$\begin{aligned} |x| + |y| + |z| &= (u + b - |z|) + (a + b - |v| - |z|) + |z| = \max\{u + b, a + b - |v|\} \\ &< \max\left\{\frac{1}{3}a + \frac{2}{3}b, \frac{2}{3}a + \frac{1}{3}b\right\} = \frac{2}{3}a + \frac{1}{3}b. \end{aligned}$$

We next show that for any N there are also integers $x, y, z \geq 0$ satisfying (16) with $x + y + z < a + b$. If $u, v \geq 0$ then $u + v \leq a + \frac{1}{2}b < a + b$ and we are done. Suppose next that $u, v \leq 0$. If $|u| \geq |v|$ then $\lambda = \mu = 0, z = |u|$ in (17) produces

$$(18) \quad x + y + z = 0 + (|u| - |v|) + |u| \leq a + b$$

since $|u| \leq \frac{1}{2}(a+b)$. Moreover, equality in (18) implies that $u = -\frac{1}{2}(a+b)$, $v = 0$ and so $c_1 = c_2 = -\frac{1}{2}$ and $0 = v = -\frac{1}{2}a$, a contradiction. Similarly if $|u| < |v| < \frac{1}{2}(a+b)$ taking $\lambda = \mu = 0$, $z = |v|$ gives

$$x + y + z = (|v| - |u|) + 0 + |v| < a + b.$$

In the remaining case $|v| \geq \frac{1}{2}(a+b)$ (and hence $c_2 < 0$, $c_1 \geq 0$ and $|u| \leq \frac{1}{2}b$.) Choosing $\lambda = 1$, $\mu = z = 0$ produces

$$x + y + z = (b - |u|) + (a + b - |v|) \leq \frac{1}{2}a + \frac{3}{2}b < a + b.$$

Suppose next that $u \leq 0$, $v \geq 0$. If $2|u| + v < a + b$ then with $\lambda = \mu = 0$, $z = |u|$,

$$x + y + z = 0 + (v + |u|) + |u| < a + b.$$

If $2|u| + v \geq a + b$ then taking $\lambda = 0$, $\mu = 1$ gives $(x, y, z) = (a - |u| + z, z - (b - v), z)$, so if $b \geq v$ letting $z = b - v$ gives

$$\begin{aligned} x + y + z &= (a + b - |u| - v) + (b - v) \leq \left(a + b - \frac{1}{2}(a + b - v) - v \right) + b - v \\ &= \frac{1}{2}a + \frac{3}{2}b - \frac{3}{2}v < a + b, \end{aligned}$$

while if $b \leq v < 2b + |u|$ choosing $\lambda = 0$, $\mu = 1$, $z = 0$ makes $x + y + z = a - b + v - |u| < a + b$. This leaves the case $2|u| + v \geq a + b$, $v - |u| \geq 2b$. Notice that in this case $c_2 > 0$ since $v > \frac{1}{2}b$ and $c_1 \leq 0$ since $u \leq 0$, so $|u| \leq \frac{1}{2}a$ and from adding the inequalities $|u| + 2v \geq a + 3b$. Taking $\lambda = -1$, $\mu = 0$ produces $(x, y, z) = (z - |u| - b, z + v - a - b, z)$, and if $|u| + v \geq a$ choosing $z = |u| + b$ gives

$$x + y + z = 0 + (|u| + v - a) + (b + |u|) \leq \left(a + \frac{b}{2} - a \right) + \left(b + \frac{a}{2} \right) = \frac{1}{2}a + \frac{3}{2}b < a + b,$$

while if $|u| + v < a$, $z = a + b - v$ has

$$x + y + z = (a - |u| - v) + 0 + (a + b - v) = 2a + b - (|u| + 2v) \leq 2a + b - (a + 3b) = a - 2b.$$

Suppose finally that $u \geq 0$, $v \leq 0$. If $2|v| + u < a + b$ then $\lambda = \mu = 0$, $z = |v|$ has $x + y + z = (u + |v|) + 0 + |v| < a + b$. If $|v| > u + b$ then $\lambda = 1$, $\mu = z = 0$ has $x + y + z = (u + b) + (a + b - |v|) + 0 < a + b$. So we may assume that $u - |v| \geq -b$ and $2|v| + u \geq a + b$ and hence, on adding that $2u + |v| > a$ (we can not have equality simultaneously since $|v| = \frac{1}{3}(a + 2b)$, $u = \frac{1}{3}(a - b)$ are not integral), so that $\lambda = 0$, $\mu = -1$, $z = a - u$ has $x = 0$, $y = a + b - |v| - u$ and

$$x + y + z = 2a + b - 2u - |v| < a + b.$$

Thus $\delta(k, p) \leq \left\lfloor \frac{2}{3}a + \frac{1}{3}b \right\rfloor = \frac{1}{3}(2a + b - \delta')$ and, for $t = 3$, $\gamma(k, p) \leq a + b - 1$. We show that these can not be reduced for the choice $N = u + vR \pmod{p}$ with

$$u = \left\lfloor \frac{1}{3}(a - b) \right\rfloor = \frac{1}{3}(a - b - \delta), \quad v = - \left\lceil \frac{1}{3}(a + 2b) \right\rceil = -\frac{1}{3}(a + 2b + \delta'),$$

where $(\delta, \delta') = (1, 2)$ or $(2, 1)$ as $a - b \equiv 1$ or $-1 \pmod{3}$ respectively. Suppose that there exist x, y, z satisfying (16) with $|x| + |y| + |z| \leq \frac{2}{3}a + \frac{1}{3}b - 1$. From (17) we have $bx + ay = bu + av + (a + b)z + \lambda p$ and so $(\lambda - \frac{1}{3})p = \frac{1}{3}(\delta b + \delta' a) + bx + ay - (a + b)z$ and

$|\lambda - \frac{1}{3}|p < \frac{2}{3}(a+b) + b|x| + a|y| + (a+b)(\frac{2}{3}a + \frac{1}{3}b - 1 - |x| - |y|) < (a+b)(\frac{2}{3}a + \frac{1}{3}b) < p$, so that $\lambda = 0$ or 1 . Moreover

$$\begin{aligned} x - y &= \frac{2}{3}a + \frac{1}{3}b + \frac{1}{3}(\delta' - \delta) - \lambda a + \mu(a+b), \\ x - z &= \frac{1}{3}a - \frac{1}{3}b - \frac{1}{3}\delta + \lambda b + \mu a, \\ y - z &= -\frac{1}{3}a - \frac{2}{3}b - \frac{1}{3}\delta' + \lambda(a+b) - \mu b \end{aligned}$$

so that when $\lambda = 0$ we have $x - y \geq \frac{2}{3}a + \frac{1}{3}b - \frac{1}{3}$ if $\mu \geq 0$ and $x - z \leq -\frac{2}{3}a - \frac{1}{3}b - \frac{1}{3}$ if $\mu \leq -1$. Similarly if $\lambda = 1$ we have $x - y \geq \frac{2}{3}a + \frac{4}{3}b - \frac{1}{3}$ if $\mu \geq 1$ and $y - z \geq \frac{2}{3}a + \frac{1}{3}b - \frac{1}{3}\delta'$ if $\mu \leq 0$. Each case contradicts $|x| + |y| + |z| \leq \frac{2}{3}a + \frac{1}{3}b - 1$.

Likewise for $x, y, z \geq 0$, $x + y + z < a + b - 1$ we have

$$\begin{aligned} \left(\lambda - \frac{1}{3}\right)p &< \frac{1}{3}(2a+b) + bx + ay < \frac{1}{3}(2a+b) + bx + a(a+b-1-x) < p \\ \left(\lambda - \frac{1}{3}\right)p &\geq -(a+b)(a+b-2) > -\frac{4}{3}p, \end{aligned}$$

and again $\lambda = 0$ or 1 . For $\lambda = 0$ we have $|x - y| > a + b$ if $\mu \geq 1$ or $\mu \leq -2$, and for $\lambda = 1$ we have $|x - y| \geq a + b$ if $\mu \leq -1$ and $x + y + z = (a + b - 1) + 3z + \mu(a - b) \geq a + b - 1$ if $\mu \geq 0$. So we are left only to check $\lambda = 0$ with $\mu = 0$ or -1 . When $\lambda = \mu = 0$, for $y \geq 0$ we must have $z \geq |v|$ and $x + y + z \geq (u + |v|) + 0 + |v| = a + b + \frac{1}{3}(2\delta' - \delta)$. When $\lambda = 0$, $\mu = -1$, for $x \geq 0$ we must have $z \geq a - u$ and $x + y + z \geq 0 + (a + b - u - |v|) + (a - u) = a + b + \frac{1}{3}(2\delta - \delta')$. \square

5. LOWER BOUNDS ON $\gamma(k, p)$

Theorem 3. *For any k, p, t we have*

$$\gamma(k, p) \geq \frac{(1 - \frac{1}{p})}{2c_t} p^{1/\phi(t)} \gg \frac{1}{\sqrt{\log t}} p^{1/\phi(t)}.$$

where

$$(19) \quad c_t = \prod_{q|t} q^{1/(2q-2)} \ll \sqrt{\log(t)},$$

the product being over the distinct odd prime divisors of t .

Proof. To begin, we identify $\mathbb{Z}/(p)$ with the residue classes from $-\frac{p-1}{2}$ to $\frac{p-1}{2}$. Let S_k be the set of nonzero k -th powers (mod p), that is, the set of t -th roots of unity. By a result of Powell [18, Theorem 3] there is a nonzero residue c (mod p) such $|cx^k| \leq c_t p^{1 - \frac{1}{\phi(t)}}$ for all nonzero x (mod p) where c_t is as given in (19). The second inequality in (19) was established in [17, p110] and [6, Theorem 2.1]. Let \bar{c} denote the multiplicative inverse of c (mod p) and suppose that $\bar{c}^{\frac{p-1}{2}}$ can be expressed as a sum of s k -th powers. Then there exist integers x_1, \dots, x_s with

$$(20) \quad cx_1^k + cx_2^k + \dots + cx_s^k \equiv \frac{p-1}{2} \pmod{p},$$

and

$$|cx_1^k + cx_2^k + \dots + cx_s^k| \leq sc_t p^{1 - \frac{1}{\phi(t)}}.$$

It follows that $s \geq (1 - \frac{1}{p})p^{1/\phi(t)}/2c_t$. \square

REFERENCES

- [1] J. Bourgain, A. Glibichuk, and S. Konyagin, *Estimates for the number of sums and products and for exponential sums in fields of prime order*, J. London Math. Soc. 73 (2006), 380-398.
- [2] J. Bourgain and S. Konyagin, *Estimates for the number of sums and products and for exponential sums over subgroups in fields of prime order*, C. R. Acad. Sci. Paris. Ser. I, 337 (2003), 75-80.
- [3] J.D. Bovey, *A new upper bound for Waring's problem (mod p)*, Acta Arith. 32 (1977) 157-162.
- [4] I. Chowla, *On Waring's problem (mod p)*, Proc. Indian Nat. Acad. Sci. A 13 (1943), 195-220.
- [5] S. Chowla, H.B. Mann and E.G. Straus, *Some applications of the Cauchy-Davenport theorem*, Norske Vid. Selsk. Forh. Trondheim 32 (1959), 74-80.
- [6] T. Cochrane, C. Pinner, and J. Rosenhouse, *Bounds on exponential sums and the polynomial Waring problem mod p*, J. London Math. Soc. (2) 67 (2003) 319-336.
- [7] M.M. Dodson, *Homogeneous additive congruences*, Philos. Trans. Roy. Soc. London, Ser. A, 261 (1967) 163-210.
- [8] ———, *On Waring's problem in $GF[p]$* , Acta Arith. 19 (1971), 147-173.
- [9] M.M. Dodson and A. Tietäväinen, *A note on Waring's problem in $GF(p)$* , Acta Arith. 19 (1971) 147-173.
- [10] C. Garcia and P. Solé, *Diameter lower bounds for Waring graphs and multiloop networks*, Discrete Math. 111 (1993), 257-261.
- [11] C. Garcia and J.F. Voloch, *Fermat curves over finite fields*, J. Number Theory 30 (1988), 345-356.
- [12] D.R. Heath-Brown and S. Konyagin, *New bounds for Gauss sums derived from k -th powers, and for Heilbronn's exponential sum*, Quart. J. Math. 51 (2000), 221-235.
- [13] G.H. Hardy and J.E. Littlewood, *Some problems of "Partitio Numerorum", VIII: The number $\Gamma(k)$ in Waring's problem*, Proc. London Math. Soc. (2) 28 (1927), 518-542.
- [14] H. Heilbronn, *Lecture Notes on Additive Number Theory mod p*, California Institute of Technology (1964).
- [15] S.V. Konyagin, *On estimates of Gaussian sums and Waring's problem for a prime modulus*, Trudy Mat. Inst. Stelov. 198 (1992) 111-124 (Russian); Proc. Steklov Inst. Math. 1 (1994) 105-117 (English trans.).
- [16] ———, *Estimates for trigonometric sums over subgroups and for Gauss sums*. (Russian) IV International Conference "Modern Problems of Number Theory and its Applications": Current Problems, Part III (Russian) (Tula, 2001), 86-114, Mosk. Gos. Univ. im. Lomonosova, Mekh.-Mat. Fak., Moscow, 2002.
- [17] S.V. Konyagin and I. Shparlinski, *Character sums with exponential functions and their applications*, Cambridge University Press 1999.
- [18] C. Powell, *Bounds for multiplicative cosets over fields of prime order*, Math. Comp. 66, no. 218, (1997), 807-822.
- [19] A. Tietäväinen, *Note on Waring's problem (mod p)*, Ann. Acad. Sci. Fenn. A I 554 (1973).
- [20] A. Weil, *Number of solutions of equations in finite fields*, Bull. AMS 55 (1949), 497-508.

DEPARTMENT OF MATHEMATICS, KANSAS STATE UNIVERSITY, MANHATTAN, KS 66506
E-mail address: `cipra@ksu.edu`

DEPARTMENT OF MATHEMATICS, KANSAS STATE UNIVERSITY, MANHATTAN, KS 66506
E-mail address: `cochrane@math.ksu.edu`

DEPARTMENT OF MATHEMATICS, KANSAS STATE UNIVERSITY, MANHATTAN, KS 66506
E-mail address: `pinner@math.ksu.edu`