JOURNAL de Théorie des Nombres de BORDEAUX

anciennement Séminaire de Théorie des Nombres de Bordeaux

Todd COCHRANE, Jeremy COFFELT et Christopher PINNER

A system of simultaneous congruences arising from trinomial exponential sums

Tome 18, n° 1 (2006), p. 59-72.

<http://jtnb.cedram.org/item?id=JTNB_2006__18_1_59_0>

Journal de Théorie des Nombres
de Bordeaux **18** (2006), 59-72

A system of simultaneous congruences arising from trinomial exponential sums

par Todd COCHRANE, Jeremy COFFELT et Christopher PINNER

Résumé. Pour p un nombre premier et $\ell < k < h < p$ des entiers positifs avec $d = (h, k, \ell, p-1)$, nous montrons que M, le nombre de solutions simultanées x, y, z, w dans $\mathbb{Z}_p^*$ de $x^h + y^h = z^h + w^h$, $x^k + y^k = z^k + w^k$, $x^\ell + y^\ell = z^\ell + w^\ell$, satisfait à

$$M \le 3d^2(p-1)^2 + 25hk\ell(p-1).$$

Quand $hk\ell = o(pd^2)$, nous obtenons un comptage asymptotique précis de M. Cela conduit à une nouvelle borne explicite pour des sommes d'exponentielles tordues

$$\left|\sum_{x=1}^{p-1} \chi(x) e^{2\pi i f(x)/p}\right| \le 3^{\frac{1}{4}} d^{\frac{1}{2}} p^{\frac{7}{8}} + \sqrt{5}\,(hk\ell)^{\frac{1}{4}}\, p^{\frac{5}{8}},$$

pour des trinômes $f = ax^h + bx^k + cx^\ell$, et à des résultats sur la valeur moyenne de telles sommes.

Abstract. For a prime p and positive integers $\ell < k < h < p$ with $d = (h, k, \ell, p-1)$, we show that M, the number of simultaneous solutions x, y, z, w in $\mathbb{Z}_p^*$ to $x^h + y^h = z^h + w^h$, $x^k + y^k = z^k + w^k$, $x^\ell + y^\ell = z^\ell + w^\ell$, satisfies

$$M \le 3d^2(p-1)^2 + 25hk\ell(p-1).$$

When $hk\ell = o(pd^2)$ we obtain a precise asymptotic count on M. This leads to the new twisted exponential sum bound

$$\left|\sum_{x=1}^{p-1} \chi(x) e^{2\pi i f(x)/p}\right| \le 3^{\frac{1}{4}} d^{\frac{1}{2}} p^{\frac{7}{8}} + \sqrt{5}\,(hk\ell)^{\frac{1}{4}}\, p^{\frac{5}{8}},$$

for trinomials $f = ax^h + bx^k + cx^\ell$, and to results on the average size of such sums.

Manuscrit reçu le 30 mars 2004.

1. Introduction

For a prime p, integer polynomial f and multiplicative character χ mod p, define the complete exponential sum

$$S(\chi, f) = \sum_{x=1}^{p-1} \chi(x) e^{2\pi i f(x)/p}.$$

Here we consider the case of trinomials

$$f = ax^h + bx^k + cx^\ell, \quad 0 < \ell < k < h < p, \ \ p \nmid abc. \tag{1.1}$$

From Weil [6]

$$|S(\chi, ax^h + bx^k + cx^\ell)| \le hp^{\frac{1}{2}},$$

and in [2] and [3] we showed the Mordell [5] type bounds

$$|S(\chi, ax^h + bx^k + cx^\ell)| \le 9^{\frac{1}{9}} (hk\ell)^{\frac{1}{9}} p^{\frac{5}{6}}, \tag{1.2}$$

$$|S(\chi, ax^h + bx^k + cx^\ell)| \le (k\ell)^{\frac{1}{4}} p^{\frac{7}{8}}. \tag{1.3}$$

Akuliničev [1] has also given a bound for a special class of trinomials.

The result (1.3) arises from the [3] bound

$$|S(\chi, ax^h + bx^k + cx^\ell)| \le p^{\frac{3}{8}} M^{\frac{1}{4}}, \tag{1.4}$$

where M denotes the number of solutions x, y, z, w in $\mathbb{Z}_p^*$ to

$$\begin{aligned} x^h + y^h &= z^h + w^h, \\ x^k + y^k &= z^k + w^k, \\ x^\ell + y^\ell &= z^\ell + w^\ell. \end{aligned}$$

It is straightforward that M is also the average value of $|S(\chi_0, f)|^4$ as a, b, c run through all of $\mathbb{Z}_p$, where χ_0 is the principal character on $\mathbb{Z}_p$. Ignoring the first equation it is not hard to show that

$$M \le (k\ell)(p-1)^2, \tag{1.5}$$

giving (1.3). Utilising the first equation we showed in [3] the slight refinement

$$M \le \frac{d}{(k,\ell)} (k\ell)(p-1)^2, \tag{1.6}$$

where

$$d = (h, k, \ell, p-1).$$

Here we obtain a more precise bound, giving an asymptotic count on M when $(hk\ell)/d^2 = o(p)$. We distinguish by M^* the number of solutions with

$$x^d = z^d, \ y^d = w^d, \text{ or } x^d = w^d, \ y^d = z^d,$$

and when $2d|(p-1)$ and $h/d, k/d, \ell/d$ are all odd

$$x^d = -y^d,\ z^d = -w^d.$$

Observe that

$$M^* = \begin{cases} 3d^2(p-1)^2 - 3d^3(p-1) & \text{if } 2d|(p-1) \text{ and } \ell/d, k/d, h/d \text{ all odd,} \\ 2d^2(p-1)^2 - d^3(p-1) & \text{otherwise.} \end{cases}$$

We show here

Theorem 1.1. *For any prime p and integers $0 < \ell < k < h < p$,*

$$0 \le M - M^* \le (17h + 8k - 19\ell)k\ell(p-1).$$

Thus, the average value of $|S(\chi_0, f)|^4$ is on the order d^2p^2 when $hk\ell \ll d^2p$. We also have the upper bound

$$M \le 3d^2(p-1)^2 + 25(hk\ell)(p-1), \tag{1.7}$$

for arbitrary h, k, ℓ. In the trivial cases $\ell = d$ and $k = 2d$ or $3d$ straightforwardly $M = M^*$. Otherwise (1.7) certainly improves upon (1.5) when $h < p/100$, and (1.6) as long as $h(k,\ell)/d < p/100$. From (1.4) and (1.7) we deduce the trinomial exponential sum bound:

Corollary 1.1. *For any trinomial* (1.1) *and multiplicative character χ* (mod p)*,*

$$|S(\chi, ax^h + bx^k + cx^\ell)| \le 3^{\frac{1}{4}} d^{\frac{1}{2}} p^{\frac{7}{8}} + \sqrt{5}(hk\ell)^{\frac{1}{4}} p^{\frac{5}{8}}.$$

The bound is nontrivial provided $d \ll p^{1/4}$ and $hk\ell \ll p^{3/2}$ and improves on the Mordell type bounds (1.2), (1.3) when $hk\ell \gg d^{9/2}p^{3/8}$, and on the Weil bound when $h \gg \max\{d^{1/2}p^{3/8}, (k\ell)^{1/3}p^{1/6}\}$. The upper bound in (1.7) is essentially best possible, although the constant 25 can likely be sharpened. The following example shows that a bound of the form

$$M - M^* \le \theta(hk\ell)(p-1)$$

can not hold with a fixed $\theta < 1$.

Lower Bound Example. For any positive integer $m \ge 5$ and prime $p \equiv 1$ (mod m), the exponents

$$\ell = 1,\ \ k = \frac{(p-1)}{m},\ \ h = \frac{2(p-1)}{m},$$

have

$$M \ge \left(1 - \frac{1}{2m}\right)(hk\ell)(p-1),$$

and hence

$$M - M^* \geq \left(1 - \frac{1}{2m} - \frac{m^2}{(p-1)}\right)(hk\ell)(p-1).$$

We prove this in Section 3.

Remark 1. If $\chi^{\frac{p-1}{d}} \neq \chi_0$ then $S(\chi, f) = 0$ for any $f = ax^h + bx^k + cx^\ell$; to see this simply replace x by $xu^{\frac{p-1}{d}}$ where $\chi^{\frac{p-1}{d}}(u) \neq 1$.

If $\chi^{\frac{p-1}{d}} = \chi_0$ then $\chi = \chi_1^d$ for some character χ_1 and we obtain the following expression for the average value of $|S(\chi, f)|^4$ over the $f = ax^h + bx^k + cx^\ell$:

$$\begin{aligned} p^{-3} \sum_{a,b,c \in \mathbb{Z}_p} |S(\chi, f)|^4 &= \sum_{\mathcal{M}} \chi(xyz^{-1}w^{-1}) \\ &= \sum_{\mathcal{M}^*} \chi_1(x^d y^d z^{-d} w^{-d}) + \sum_{\mathcal{M} - \mathcal{M}^*} \chi(xyz^{-1}w^{-1}) \\ &= 2d^2(p-1)^2 + 25\theta hk\ell p \end{aligned}$$

with $|\theta| \leq 1$, unless $2d|(p-1)$, ℓ/d, k/d, h/d are all odd, and $\chi^2 = \chi_0$, in which case the constant 2 on the right is replaced by 3; here $\mathcal{M}$ and $\mathcal{M}^*$ are the sets of points contributing to M and M^* respectively.

Using the Hölder inequality,

$$N^{-1}\left(\sum_{i=1}^N a_i\right)^2 \leq \sum_{i=1}^N a_i^2 \leq \left(\sum_{i=1}^N a_i\right)^{2/3}\left(\sum_{i=1}^N a_i^4\right)^{1/3},$$

and the fact that

$$p^{-3} \sum_{a,b,c \in \mathbb{Z}_p} |S(\chi, f)|^2 = d(p-1),$$

for $\chi^{\frac{p-1}{d}} = \chi_0$, we obtain the following estimate for the average value of $|S(\chi, f)|$:

(1.8)

$$\frac{1}{\sqrt{2}}\sqrt{d(p-1)}\left(1 - \frac{25hk\ell p}{4d^2(p-1)^2}\right) \leq p^{-3} \sum_{a,b,c \in \mathbb{Z}_p} |S(\chi, f)| \leq \sqrt{d(p-1)}$$

for $hk\ell \ll d^2 p$. Again the constant $\frac{1}{\sqrt{2}}$ on the left must be replaced by $\frac{1}{\sqrt{3}}$ in the exceptional case mentioned above.

Remark 2. By Weil's fundamental work we know that $S(\chi, f) = -\omega_1 - \cdots - \omega_h$ for some complex numbers ω_i, each of modulus $\sqrt{p}$, and so if the arguments of the ω_i are randomly distributed one might expect an upper bound of the type $|S(\chi, f)| \ll (hp)^{\frac{1}{2}+\epsilon}$. It is interesting to note that upper bounds of the type (1.3) and Corollary 1.1 are actually much sharper than

this bound for large classes of trinomials. For instance, from (1.3) we have the uniform upper bound,

$$|S(\chi, ax^h + bx^2 + cx)| \le 2^{1/4}p^{7/8},$$

which is sharper than $\sqrt{hp}$ for $h \gg p^{3/4}$. It would be of interest to understand how the extra cancellation in the sum of the ω_i is occurring in such cases.

2. Proof of Theorem 1

Dividing by w we can clearly write $M = (p-1)|M_0|$ where M_0 denotes the solutions x, y, z in $\mathbb{Z}_p^*$ to

$$\begin{aligned} x^h + y^h - z^h - 1 &= 0, \\ x^k + y^k - z^k - 1 &= 0, \\ x^\ell + y^\ell - z^\ell - 1 &= 0. \end{aligned} \tag{2.1}$$

We write M_0^* for the solutions to (2.1) with

$$x^h = x^k = x^\ell = 1,\ y^h = z^h, y^k = z^k, y^\ell = z^\ell,$$

or

$$y^h = y^k = y^\ell = 1, x^h = z^h, x^k = z^k, x^\ell = z^\ell,$$

or

$$x^h = -y^h, x^k = -y^k, x^\ell = -y^\ell, z^h = z^k = z^\ell = -1,$$

the last of these contributing no solutions unless $h/d, k/d, \ell/d$ are all odd and $(p-1)/d$ is even. Straightforwardly these correspond to solutions with respectively $x^d = 1$, $y^d = z^d$, or $y^d = 1$, $x^d = z^d$, or $z^d = -1$, $x^d = -y^d$, and hence $M^* = |M_0^*|(p-1)$.

We recall Theorem 1 of Wooley [7]: If $f_i(x_1, ..., x_k)$ are polynomials in $\mathbb{Z}[x]$ of degree d_i, then the number of simultaneous solutions $x_1, ..., x_k$ in $\mathbb{Z}_p$ to $f_i(x_1, ..., x_k) = 0$, $i = 1, ..., k$ with $\det\left(\frac{\partial f_i}{\partial x_j}\right) \neq 0$ is bounded by $d_1 \cdots d_k$.

Hence we have

$$M - M^* \le (hk\ell)(p-1) + |M_1|(p-1)$$

where M_1 denotes the solutions to (2.1), not in M_0^*, and with

$$\begin{aligned} \frac{xyz}{hk\ell} \det \begin{pmatrix} hx^{h-1} & hy^{h-1} & -hz^{h-1} \\ kx^{k-1} & ky^{k-1} & -kz^{k-1} \\ \ell x^{\ell-1} & \ell y^{\ell-1} & -\ell z^{\ell-1} \end{pmatrix} &= \det \begin{pmatrix} x^h & y^h & -z^h \\ x^k & y^k & -z^k \\ x^\ell & y^\ell & -z^\ell \end{pmatrix} \\ &= \det \begin{pmatrix} x^h & y^h & 1 \\ x^k & y^k & 1 \\ x^\ell & y^\ell & 1 \end{pmatrix} = 0 \end{aligned}$$

Thus for these solutions we obtain the additional equation

$$F_1 := x^h(y^k - y^\ell) + x^k(y^\ell - y^h) + x^\ell(y^h - y^k) = 0. \tag{2.2}$$

Since $z^k = x^k + y^k - 1$ and $z^\ell = x^\ell + y^\ell - 1$ the solutions to (2.1) must also satisfy

$$F_2 := (x^k + y^k - 1)^{\ell/e} - (x^\ell + y^\ell - 1)^{k/e} = 0$$

where $e = (\ell, k)$. Observe that for a given pair x, y the number of solutions (x, y, z) is at most d (we obtain z^h, z^k, z^ℓ and hence z^d from (2.1)). Thus applying Wooley again to the pair $(xy)^{-\ell}F_1$, F_2 we obtain that

$$|M_1| \le (h + k - 2\ell)\frac{k\ell}{e}d + |M_2|$$

where M_2 denotes the solutions in M_1 which additionally have

$$\det \begin{pmatrix} x\frac{\partial F_1}{\partial x} & y\frac{\partial F_1}{\partial y} \\ x\frac{\partial F_2}{\partial x} & y\frac{\partial F_2}{\partial y} \end{pmatrix} = 0. \tag{2.3}$$

To avoid rewriting the same expressions we define the following polynomials in y:

$$\Delta := y^k - y^\ell \tag{2.4}$$

and

(2.5)

$$U := (h-k)(y^h - y^\ell), \quad H := (k-h)y^{k+h} + (\ell - k)y^{k+\ell} + (h-\ell)y^{h+\ell},$$
$$V := (\ell - h)(y^h - y^k), \quad L := (k-\ell)y^h - (h-\ell)y^k + (h-k)y^\ell,$$

and, noting the highest and lowest degree terms,

$$\begin{aligned} A &:= (y^\ell - 1)H + y^\ell U\Delta \\ &= (h-k)y^{k+h} + (k-\ell)y^{h+2\ell} + \cdots + (k-\ell)y^{k+\ell} + (h-k)y^{3\ell}, \\ B &:= -(y^k - 1)H - y^k U\Delta \\ &= -(y^\ell - 1)H + y^\ell V\Delta = -(k-\ell)y^{h+k+\ell} + \cdots - (k-\ell)y^{k+\ell}, \\ C &:= (y^k - 1)H - y^k V\Delta = (k-\ell)y^{2k+h} + \cdots + (k-\ell)y^{\ell+k}. \end{aligned} \tag{2.6}$$

We note the relations

$$Vy^\ell + Uy^k + H = 0, \tag{2.7}$$

$$Ay^{k-\ell} + B(1 + y^{k-\ell}) + C = 0, \tag{2.8}$$

and

(2.9)

$$B^2 - AC = (A+B)(Ay^{k-\ell} + B), \quad A + B = -\Delta L y^\ell, \quad B + Ay^{k-\ell} = -\Delta H y^{-\ell},$$

as can be readily checked using Maple. Using the relation $F_1 = 0$ we have

$$\begin{aligned} x\frac{\partial F_1}{\partial x} &= hx^h(y^k - y^\ell) + kx^k(y^\ell - y^h) + \ell x^\ell(y^h - y^k) \\ &= x^k U + x^\ell V, \end{aligned}$$

$$\begin{aligned} \Delta y\frac{\partial F_1}{\partial y} &= (y^k - y^\ell)\left(x^h(ky^k - \ell y^\ell) + x^k(\ell y^\ell - hy^h) + x^\ell(hy^h - ky^k)\right) \\ &= x^k\left((y^k - y^\ell)(\ell y^\ell - hy^h) - (y^\ell - y^h)(ky^k - \ell y^\ell)\right) \\ &\quad + x^\ell\left((y^k - y^\ell)(hy^h - ky^k) - (y^h - y^k)(ky^k - \ell y^\ell)\right) \\ &= (x^k - x^\ell)H. \end{aligned}$$

Using that $z^k = x^k + y^k - 1$ and $z^\ell = x^\ell + y^\ell - 1$ gives

$$\begin{aligned} x\frac{\partial F_2}{\partial x} &= \frac{\ell}{e}(x^k + y^k - 1)^{\frac{\ell}{e}-1}kx^k - \frac{k}{e}(x^\ell + y^\ell - 1)^{\frac{k}{e}-1}\ell x^\ell \\ &= \frac{k\ell}{e}\frac{z^{k\ell/e}}{(x^k + y^k - 1)(x^\ell + y^\ell - 1)} \\ &\quad \times \left(x^k(x^\ell + y^\ell - 1) - x^\ell(x^k + y^k - 1)\right) \\ &= \frac{k\ell}{e}z^{k\ell/e-k-\ell}\left(z^k(y^\ell - 1) - z^\ell(y^k - 1)\right), \end{aligned}$$

$$\begin{aligned} \Delta y\frac{\partial F_2}{\partial y} &= \Delta\frac{k\ell}{e}\frac{z^{k\ell/e}}{(x^k + y^k - 1)(x^\ell + y^\ell - 1)} \\ &\quad \times \left(y^k(x^\ell + y^\ell - 1) - y^\ell(x^k + y^k - 1)\right) \\ &= -\frac{k\ell}{e}z^{k\ell/e-k-\ell}\Delta\left(z^k y^\ell - z^\ell y^k\right). \end{aligned}$$

Thus we obtain from the determinant (2.3) that

(2.10)
$$\left(z^k(y^\ell - 1) - z^\ell(y^k - 1)\right)(x^k - x^\ell)H + \Delta\left(x^k U + x^\ell V\right)\left(z^k y^\ell - z^\ell y^k\right) = 0.$$

Dividing by $(xz)^\ell$, and using (2.6) for the coefficients obtained, gives one more equation

$$F_3 := A(xz)^{k-\ell} + B(x^{k-\ell} + z^{k-\ell}) + C = 0. \tag{2.11}$$

From (2.8) this can also be written

$$F_3 = A((xz)^{k-\ell} - y^{k-\ell}) + B(x^{k-\ell} + z^{k-\ell} - 1 - y^{k-\ell}) = 0. \tag{2.12}$$

Notice that the solutions in M_0^* with $\Delta \neq 0$ have $\{x^{k-\ell}, z^{k-\ell}\} = \{1, y^{k-\ell}\}$. These are precisely the solutions to (2.12) which are independent of the y

dependence A, B. From (2.11) we obtain the relation

$$z^{k-\ell}(Ax^{k-\ell}+B) = -(Bx^{k-\ell}+C). \tag{2.13}$$

From (2.6) it is clear that $y^{\ell+\min\{k,2\ell\}}$ divides F_3. Applying Wooley again to $F_3/y^{\ell+\min\{k,2\ell\}}$, $x^k+y^k-z^k-1$, $x^\ell+y^\ell-z^\ell-1$, we obtain:

$$|M_2| \le (h+k-5\ell+2\max\{k,2\ell\})k\ell + |M_3| + |M_4|$$

where M_3, M_4 are solutions M_2 with

$$\det\begin{pmatrix} \frac{x}{(k-\ell)}\frac{\partial F_3}{\partial x} & -\frac{z}{(k-\ell)}\frac{\partial F_3}{\partial z} & \frac{y}{(k-\ell)}\frac{\partial F_3}{\partial y} \\ x^k & z^k & y^k \\ x^\ell & z^\ell & y^\ell \end{pmatrix} = 0, \tag{2.14}$$

with $\Delta(Ax^{k-\ell}+B)=0$ for M_3 and $\Delta(Ax^{k-\ell}+B)\neq 0$ for M_4. Observe that for each y there will be at most $k\ell/e$ values of x (using $F_2=0$ as long as at least one of y^k-1 and $y^\ell-1$ is non-zero, and using $F_1=0$ to obtain $x^{k-\ell}=1$ when $y^k=y^\ell=1$ and $y^h\neq 1$ since we are not in M_0^*). If $Ax^{k-\ell}+B=0$, then $Bx^{k-\ell}+C=0$ and, eliminating $x^{k-\ell}$ we obtain $B^2-AC=0$. From (2.9) this gives $\Delta HL=0$ and the number of values of y in M_3 is at most $(k-\ell)+(h-\ell)+(h-\ell)$. Hence

$$|M_3| \le (2h+k-3\ell)\frac{k\ell}{e}d.$$

For M_4 observe from (2.12) that if $x^{k-\ell}=1$ then $z^{k-\ell}=y^{k-\ell}$ (we know that $A+B\neq 0$ else we would be in M_3). Since $y^{k-\ell}\neq 1$ in M_4, the relations

$$z^\ell = \frac{x^{k-\ell}(y^\ell-1)-(y^k-1)}{x^{k-\ell}-z^{k-\ell}}, \quad x^\ell = \frac{z^{k-\ell}(y^\ell-1)-(y^k-1)}{x^{k-\ell}-z^{k-\ell}}, \tag{2.15}$$

arising from the k and ℓ equations of (2.1), then give $z^\ell=y^\ell$, $x^\ell=1$, $z^k=y^k$, $x^k=1$. But from $F_1=\Delta(x^h-1)=0$ this forces $x^h=1$, $y^h=z^h$ and we obtain no solutions not in M_0^*. Likewise if $x^{k-\ell}=y^{k-\ell}$ then $Ay^{k-\ell}+B\neq 0$ and $z^{k-\ell}=1$, and $z^\ell=-1$, $z^k=-1$, $x^\ell=-y^\ell$, $x^k=-y^k$, and $F_1=\Delta(x^h+y^h)=0$ giving $x^h=-y^h$, and we obtain no solutions not in M_0^*.

Hence, writing $X=x^{k-\ell}$, $Y=y^{k-\ell}$, we may assume henceforth for points in M_4 that

$$X\neq 1, \qquad X\neq Y \quad \text{and} \quad k\neq 2\ell. \tag{2.16}$$

The assumption $k\neq 2\ell$ follows from the observation that if $k=2\ell$ then $(x^\ell-1)(y^\ell-1)=1$ (as in (3.1)) and so either $X=1$ or $Y=1$, the latter implying $\Delta=0$ whence we are in M_3. Defining $A_1 := \frac{y}{(k-\ell)}\frac{\partial A}{\partial y}$, $B_1 := \frac{y}{(k-\ell)}\frac{\partial B}{\partial y}$, $C_1 := \frac{y}{(k-\ell)}\frac{\partial C}{\partial y}$, using (2.13) to eliminate $z^{k-\ell}$, and invoking

relation (2.9), we have

$$\frac{x}{(k-\ell)}\frac{\partial F_3}{\partial x} = A(xz)^{k-\ell} + Bx^{k-\ell} = \frac{(B^2-AC)X}{AX+B} = \frac{HL\Delta^2 X}{AX+B}$$
$$-\frac{z}{(k-\ell)}\frac{\partial F_3}{\partial z} = -(A(xz)^{k-\ell} + Bz^{k-\ell}) = BX + C,$$

and using successively (2.8), (2.13) to eliminate $z^{k-\ell}$ and (2.8) again,

$$\begin{aligned}-\frac{y}{(k-\ell)}\frac{\partial F_3}{\partial y} &= A_1(xz)^{k-\ell} + B_1(x^{k-\ell} + z^{k-\ell}) + C_1\\ &= A_1((xz)^{k-\ell} - y^{k-\ell}) + B_1(x^{k-\ell} + z^{k-\ell} - 1 - y^{k-\ell})\\ &\quad + (B+C)\\ &= (B_1A - BA_1)\frac{(X-1)(X-Y)}{AX+B} + (B+C).\end{aligned}$$

Thus from the determinant condition (2.14), and writing $Xz^\ell - z^k = X(y^\ell - 1) - (y^k - 1)$, we see that

$$-HL\Delta^2 X\left(\frac{z^k y^\ell - z^\ell y^k}{x^\ell}\right)$$

equals

$$\begin{aligned}&-(BX+C)(AX+B)(Xy^\ell - y^k) + [(B_1A - A_1B)(X-1)(X-Y)\\ &\quad +(B+C)(AX+B)]\left(X(y^\ell-1) - (y^k-1)\right)\\ &= (X-1)\left[(B_1A - A_1B)(X-Y)\left(X(y^\ell-1) - (y^k-1)\right)\right.\\ &\quad \left.-(AX+B)\left(By^\ell(X-Y) + (B+C)\right)\right],\end{aligned}$$

while from (2.10)

$$-\Delta(XU+V)\left(\frac{z^k y^\ell - z^\ell y^k}{x^\ell}\right) = H(X-1)(X(y^\ell-1) - (y^k-1)).$$

Thus since $X \neq 1$ we must have $T_1 = T_2$ where

$$T_1 := H^2 L\Delta X\left(X(y^\ell-1) - (y^k-1)\right)$$

and, using from (2.8) and (2.9) that $-(B+C)(AY+B) = Y(A+B) \times (AY+B) = YHL\Delta^2$,

$$\begin{aligned} T_2 &:= (XU+V)\Big[(B_1A-A_1B)(X-Y)\Big(X(y^\ell-1)-(y^k-1)\Big)\\ &\qquad -(AX+B)\Big(By^\ell(X-Y)+(B+C)\Big)\Big]\\ &= (XU+V)\Big\{(X-Y)\Big[(B_1A-A_1B)(X(y^\ell-1)-(y^k-1))\\ &\qquad -By^\ell(AX+B)-(B+C)A\Big]+YHL\Delta^2\Big\}. \end{aligned}$$

Now

$$T_1 = H^2L\Delta X\Big((y^\ell-1)(X-Y)-y^{-\ell}\Delta\Big) = (X-Y)T_3 - H^2L\Delta^2Yy^{-\ell}$$

with

$$T_3 := H^2L\Delta\Big((y^\ell-1)X-y^{-\ell}\Delta\Big).$$

Also, using (2.7),

$$T_2 = (X-Y)T_4 - H^2L\Delta^2Yy^{-\ell}$$

with

$$\begin{aligned} T_4 &:= \Big[(B_1A-A_1B)\Big(X(y^\ell-1)-(y^k-1)\Big)\\ &\qquad -By^\ell(AX+B)-(B+C)A\Big](XU+V)+YHL\Delta^2U\\ &= \Delta(aX-b)(XU+V)+YHL\Delta^2U \end{aligned}$$

where

$$\begin{aligned} a &:= \Big((B_1A-A_1B)(y^\ell-1)-ABy^\ell\Big)/\Delta,\\ b &:= \Big((B_1A-A_1B)(y^k-1)+B^2y^\ell+(B+C)A\Big)/\Delta \end{aligned}$$

(one can verify by Maple that a and b are polynomials). Since $X \neq Y$ we obtain $T_3 = T_4$, a quadratic relation in X, and after multiplying by $(k-\ell)$,

$$\alpha x^{2(k-\ell)} + \beta x^{k-\ell} + \gamma = 0, \tag{2.17}$$

with (using Maple to expand and identify the highest and lowest degree terms)

$$\begin{aligned} \alpha &:= (k-\ell)Ua = (h-k)^2(k-\ell)(k-2\ell)y^{k+4\ell}(y^{3h-2\ell}+\cdots+1),\\ \beta &:= (k-\ell)(Va-Ub-H^2L(y^\ell-1))\\ &= -(h-k)^2(k-\ell)(k-2\ell)y^{k+4\ell}\Big(y^{3h+k-3\ell}+\cdots+1\Big),\\ \gamma &:= (k-\ell)(-Vb+H^2L\Delta y^{-\ell}+YHLU\Delta)\\ &= (h-\ell)\ell(k-h)(k-\ell)y^{3\ell+2k}(y^{3h-2\ell}+\cdots+1). \end{aligned}$$

Observing that $B\beta = C\alpha + A\gamma$ (as can be checked on Maple), the relation (2.13) and quadratic (2.17) yield the equations

$$F_4 := \alpha(xz)^{k-\ell} - \gamma = 0 \tag{2.18}$$

and

$$\alpha\left(x^{k-\ell} + z^{k-\ell}\right) = -\beta. \tag{2.19}$$

One can use Maple to obtain explicit expressions for the polynomials α and γ

$$\begin{aligned}\alpha &= (h-k)(y^h - y^\ell)y^\ell f(h,k,\ell),\\ \gamma &= (h-\ell)(y^h - y^k)y^\ell f(h,\ell,k),\end{aligned}$$

with

$$\begin{aligned}f(h,k,\ell) = {}& (k-\ell)(h-k)(k-2\ell)\left(y^{2h+k+\ell} - y^{k+2\ell}\right)\\ &+ k(h-\ell)(k-\ell)\left(y^{2h+2\ell} - y^{2k+\ell}\right)\\ &+ (2h^3 + 2k^3 + 14hk\ell - k\ell^2 - h\ell^2 - 3hk^2 - 3h^2k\\ &\quad - 5h^2\ell - 5k^2\ell)\left(y^{h+k+2\ell} - y^{h+k+\ell}\right)\\ &+ h(h-\ell)(k-\ell)\left(y^{2k+2\ell} - y^{2h+\ell}\right)\\ &+ (2\ell - h)(h-\ell)(h-k)\left(y^{h+2k+\ell} - y^{h+2\ell}\right)\\ &+ (\ell + k - h)(h-\ell)(h-k)\left(y^{h+3\ell} - y^{h+2k}\right)\\ &- (h + \ell - k)(h-k)(k-\ell)\left(y^{k+3\ell} - y^{2h+k}\right).\end{aligned}$$

Thus applying Wooley again to $F_4/y^{k+4\ell}$, $x^k + y^k - z^k - 1$, $x^\ell + y^\ell - z^\ell - 1$, we have

$$|M_4| \le (3h + 2k - 4\ell)k\ell + |M_5|$$

where solutions in M_5 have an additional zero determinant (of the form (2.14) with F_4 in place of F_3).

Writing $\alpha_1 = \frac{y}{(k-\ell)}\frac{\partial\alpha}{\partial y}$, $\gamma_1 = \frac{y}{(k-\ell)}\frac{\partial\gamma}{\partial y}$, we have

$$\begin{aligned}\frac{\alpha x}{(k-\ell)}\frac{\partial F_4}{\partial x} &= \alpha^2(xz)^{k-\ell} = \gamma\alpha,\\ -\frac{\alpha z}{(k-\ell)}\frac{\partial F_4}{\partial z} &= -\alpha^2(xz)^{k-\ell} = -\gamma\alpha,\\ \frac{\alpha y}{(k-\ell)}\frac{\partial F_4}{\partial y} &= \alpha(\alpha_1(xz)^{k-\ell} - \gamma_1) = \alpha_1\gamma - \alpha\gamma_1,\end{aligned}$$

and thus for solutions in M_5 we gain the relation

$$\alpha\gamma\left((z^k y^\ell - z^\ell y^k) + (x^k y^\ell - x^\ell y^k)\right) + (\alpha_1\gamma - \alpha\gamma_1)(x^k z^\ell - x^\ell z^k) = 0. \tag{2.20}$$

When $z^{k-\ell} \neq x^{k-\ell}$ and $\alpha \neq 0$ we use (2.15) to rewrite $(z^k y^\ell - z^\ell y^k) + (x^k y^\ell - x^\ell y^k)$ as

$$\begin{aligned} & z^\ell x^\ell \left(\frac{z^{k-\ell} y^\ell - y^k}{x^\ell} + \frac{x^{k-\ell} y^\ell - y^k}{z^\ell} \right) \\ & = (x^k z^\ell - z^k x^\ell) \left(\frac{z^{k-\ell} y^\ell - y^k}{z^{k-\ell}(y^\ell - 1) - (y^k - 1)} + \frac{x^{k-\ell} y^\ell - y^k}{x^{k-\ell}(y^\ell - 1) - (y^k - 1)} \right) \\ & = (x^k z^\ell - z^k x^\ell) \frac{T_5}{T_6} \end{aligned}$$

where using (2.18) and (2.19)

$$\begin{aligned} T_5 &:= 2\gamma y^\ell (y^\ell - 1) + \beta(y^k(y^\ell - 1) + y^\ell(y^k - 1)) + 2\alpha y^k (y^k - 1), \\ T_6 &:= \gamma(y^\ell - 1)^2 + \beta(y^\ell - 1)(y^k - 1) + \alpha(y^k - 1)^2. \end{aligned}$$

Thus, by (2.20)

$$F_5 := \alpha\gamma T_5 + (\alpha_1\gamma - \alpha\gamma_1) T_6 = 0,$$

a relation which only depends upon the variable y.

If $\alpha = 0$ then $\gamma = 0$ (from (2.18) both are zero or non-zero) and y will still be a zero of F_5. If $z^{k-\ell} = x^{k-\ell}$ and $\alpha \neq 0$ then from (2.19) and (2.18)

$$x^{k-\ell} = -\beta/2\alpha, \quad \beta^2 - 4\alpha\gamma = 0, \tag{2.21}$$

while (2.20) gives $\alpha\gamma\left(z^\ell + x^\ell\right)(x^{k-\ell} y^\ell - y^k) = 0$ and, since $x^{k-\ell} \neq y^{k-\ell}$, we must have $x^\ell = -z^\ell$, $x^k = -z^k$, and $2x^k = 1 - y^k$, $2x^\ell = 1 - y^\ell$. Hence $T_6 = 4x^{2\ell}(\gamma + \beta x^{k-\ell} + \alpha x^{2(k-\ell)}) = 0$ by (2.17), and $T_5 = 8x^{2\ell}(\gamma + \beta x^{k-\ell} + \alpha x^{2(k-\ell)}) - 2x^\ell\left(2\gamma + \beta(1 + x^{k-\ell}) + 2\alpha x^{k-\ell}\right) = 0$, by (2.17) and (2.21), and these solutions are also included in $F_5 = 0$. Hence all solutions in M_5 have y value satisfying $F_5 = 0$, where for each y there are at most $\frac{k\ell}{e} d \leq k\ell$ choices of x and z as we saw in the bound for M_3.

Again appealing to Maple we obtain

$$F_5 = -\ell(\ell - h)(k - h)^5 (2\ell - k)(\ell - k)^3 (\ell + h - k)\Delta y^{4k+11\ell}\left(y^{9h+k-7\ell} + \cdots + 1\right)$$

a nonzero polynomial by our assumption (2.16). Since the values where $\Delta = 0$ are already accounted for in M_3 and for each choice of y there are at most $k\ell$ choices for (x, z) (as noted above in the estimate for $|M_3|$) we have finally

$$|M_5| \leq (9h + k - 7\ell)k\ell,$$

and

$$M - M^* \leq (17h + 8k - 19\ell)k\ell(p - 1).$$

3. Proof for the Example.

Let m be a positive integer with $m \geq 5$, p a prime with $p \equiv 1 \pmod{m}$, and $(h, k, \ell) = (2(p-1)/m, (p-1)/m, 1)$.

Clearly $M = (p-1)M_0$ where M_0 counts the solutions x, y, z in $\mathbb{Z}_p^*$ to

$$x^k + y^k = z^k + 1, \quad x^{2k} + y^{2k} = z^{2k} + 1, \quad x + y = z + 1. \tag{3.1}$$

From the first two equations we have $z^k = x^k y^k$ and $(x^k - 1)(y^k - 1) = 0$ and so $x^k = 1$, $y^k = z^k$ or $y^k = 1$, $x^k = z^k$. Now if $x^k = 1$, $y^k = z^k$ then $y = \xi z$ for the k values ξ with $\xi^k = 1$, the remaining equation requiring $(x + z\xi) = (z + 1)$. Thus for $\xi = 1$ we have the $(p-1)$ solutions $x = 1$, $z = y$, and for the $(k-1)$ remaining $\xi \neq 1$ we have solutions $z = (x-1)/(1-\xi)$, $y = \xi z$ for the $(k-1)$ values of $x \neq 1$ with $x^k = 1$. A similar count is obtained when $y^k = 1$ and $x^k = z^k$. Hence

$$M_0 = 2(p-1) + 2(k-1)^2 - M'$$

where M' is the number of solutions to $x + y = z + 1$ with $x^k = y^k = z^k = 1$, so that $m^3 M'$ equals the number of solutions to $x^m + y^m = z^m + 1$. By Theorem 6.37 of [4]

$$m^3 M' \leq p^2 + (m-1)^3 p,$$

and, for $m \geq 5$,

$$M_0 \geq 2(k-1)^2 + 2(p-1) - p^2/m^3 - p > \left(2 - \frac{1}{m}\right) k^2.$$

References

[1] N. M. Akuliničev, *Estimates for rational trigonometric sums of a special type.* Doklady Acad. Sci. USSR **161** (1965), 743–745. English trans in Doklady **161**, no. 4 (1965), 480–482.

[2] T. Cochrane & C. Pinner, *An improved Mordell type bound for exponential sums.* Proc. Amer. Math. Soc. **133** (2005), 313–320.

[3] T. Cochrane, J. Coffelt & C. Pinner, *A further refinement of Mordell's bound on exponential sums.* Acta Arith. **116** (2005), 35–41.

[4] R. Lidl & H. Niederreiter, *Finite Fields.* Encyclopedia of mathematics and its applications, Addison-Wesley, 1983.

[5] L. J. Mordell, *On a sum analogous to a Gauss's sum.* Quart. J. Math. **3** (1932), 161–167.

[6] A. Weil, *On some exponential sums.* Proc. Nat. Acad. Sci. U.S.A. **34** (1948), 204–207.

[7] T. Wooley, *A note on simultaneous congruences.* J. Number Theory **58** (1996), no. 2, 288–297.

Todd Cochrane
Department of Mathematics
Kansas State University
Manhattan, KS 66506, USA
E-mail: cochrane@math.ksu.edu
URL: http://www.math.ksu.edu/~cochrane

Jeremy Coffelt
Department of Mathematics
Kansas State University
Manhattan, KS 66506, USA
E-mail: jcoffelt@math.ksu.edu

Christopher Pinner
Department of Mathematics
Kansas State University
Manhattan, KS 66506, USA
E-mail: pinner@math.ksu.edu
URL: http://www.math.ksu.edu/~pinner/