Permutations of even residues modulo p

Todd Cochrane Jennifer Paulhus Christopher Pinner

(Jean Bourgain)

Kansas State University
paulhus@math.ksu.edu
www.math.ksu.edu/∼paulhus

Notation

For this talk

- $p > 13$ a prime
- A, d integers where $(d, p-1) = 1$ and $p \nmid A$
- $\mathbb{E}$ the set of even residues mod p, $\mathbb{E} = \{2, 4, 6, \ldots, p-1\}$
- $\mathbb{O}$ the set of odd residues mod p, $\mathbb{O} = \{1, 3, 5, \ldots, p-2\}$

We want to determine when the map $x \to Ax^d$ is a permutation of the elements of $\mathbb{E}$ (i.e. when $A\mathbb{E}^d \cap \mathbb{O}$ is empty).

Besides the trivial case ($d = A = 1$) the following 6 cases also give permutations of $\mathbb{E}$:

$(p, A, d) = (5, 3, 3), (7, 1, 5), (11, 9, 3), (11, 3, 7), (11, 5, 9), (13, 1, 5).$

We can assume $0 < |A| < p/2$ and $|d| < p/2$.

Conjecture (Goresky and Klapper, 1997)

If 2 is a primitive root modulo p, with the exception of the six cases listed before, if $(A, d) \neq (1, 1)$ *then* $A\mathbb{E}^d \cap \mathbb{O}$ *is nonempty.*

Goresky, Klapper, Murty, and Shparlinski verified the conjecture for primes p less than 2 million. And for the following cases:

1. $d = -1$
2. $p \equiv 1 \bmod 4$ and $d = \frac{p+1}{2}$
3. $1 < d \leq \frac{(p^2-1)^4}{2^{16} p^7 (\ln(q)+2)^4}$

They subsequently improved (3) to $d \leq \frac{(p^2-1)^4}{2^{25} p^7}$.

It was suggested by Bourgain that exponential sum bounds of Cochrane and Pinner could be used to solve this conjecture for sufficiently large primes.

Motivation

Definition

Given a prime p and $A \in \mathbb{Z}/p\mathbb{Z}$, an ℓ**-sequence** based on p is a sequence $\{a_i\}_i$ of 0's and 1's with $a_i \equiv (A2^{-i} \bmod p) \bmod 2$.

These sequences are strictly periodic with period $p - 1$ when 2 is a primitive root mod p.

- 2-adic expansion of a rational number r/p with $(r, p) = 1$
- Single codeword in the Barrows-Mandelbaum arithmetic code
- Output sequence from maximal period feedback with carry shift register

Definition

If **a** is an ℓ-sequence based on p then if $(d, p-1) = 1$, an **allowable decimation** of **a** is the sequence $\mathbf{x} = \mathbf{a^d} = \{a_{d \cdot i}\}_i$.

Definition

Two periodic binary sequences **a** and **b** with the same period T are **cyclically distinct** if $\mathbf{a_t} \neq \mathbf{b}$ for all $0 < t < T$, where $\mathbf{a_t} = \{a_{i+t}\}_i$.

Conjecture (Goresky and Klapper, 1997)

If $p > 13$ is a prime such that 2 is a primitive root mod p and **a** *is an ℓ-sequence based on p, then every pair of allowable decimations of* **a** *is cyclically distinct.*

This conjecture would give many distinct sequences with **ideal arithmetic cross-correlation**.

Conjecture

If $p > 13$ is a prime such that 2 is a primitive root mod p and **a** *is an ℓ-sequence based on p, then every pair of allowable decimations of* **a** *is cyclically distinct.*

a is a cyclic permutation of $\mathbf{a^d}$ if and only if there exists
$A \in (\mathbb{Z}/p\mathbb{Z})^\times$ with $(A2^{-id} \bmod p) \equiv (2^{-i} \bmod p) \bmod 2$ for all i
if and only if $(Ax^d \bmod p) \equiv (x \bmod p) \bmod 2$ for all x.

Note: We need 2 to be a primitive root for the second equivalence.

Conjecture

If 2 is a primitive root modulo p, with the exception of the six cases listed before, if $(A, d) \neq (1, 1)$ then $A\mathbb{E}^d \cap \mathbb{O}$ is nonempty.

Theorem (Cochrane, P., Pinner)

For $p > 4.29 \cdot 10^{68}$ and $(A, d) \neq (1, 1)$, $A\mathbb{E}^d \cap \mathbb{O}$ is nonempty.

To show $A\mathbb{E}^d \cap \mathbb{O}$ is nonempty, we find a solution (x, y) to the equation $A(2x)^d = 2y - 1$ with $(x, y) \in I_1 \times I_2$ where

$$I_1 = \{0, 1, 2, \ldots, \frac{p-1}{2}\}$$

$$I_2 = I_1 - \{0\}.$$

Additive Character Approach

$$I_3 = \left\{0, 1, 2, \ldots, \left\lfloor \frac{p-1}{4} \right\rfloor \right\} \text{ and } I_4 = \left\{1, 2, \ldots, \left\lfloor \frac{p+1}{4} \right\rfloor \right\}$$

so that $I_3 + I_3 \subset I_1$ and $I_3 + I_4 \subset I_2$. Let α be the convolution

$$\alpha(x, y) = \chi_{I_3} * \chi_{I_3}(x) \cdot \chi_{I_3} * \chi_{I_4}(y).$$

χ_I is the characteristic function of an interval I.

We let $e_p(\star)$ be the additive character $e^{2\pi i \star / p}$. The Fourier expansion of $\alpha(x, y)$ is $\sum a(u, v) e_p(ux + vy)$.

α is supported on $I_1 \times I_2$ so enough to show

$$\sum_{\substack{A(2x)^d = 2y-1 \\ x \neq 0}} \alpha(x, y) > 0$$

$$\sum_{\substack{A(2x)^d = 2y-1 \\ x \neq 0}} \alpha(x, y) = \sum_{\substack{A(2x)^d = 2y-1 \\ x \neq 0}} \sum_{u,v} a(u, v) e_p(ux + vy) = a(0, 0)(p-1) +$$

$$\sum_{(u,v) \neq (0,0)} a(u, v) e_p(2^{-1} v) \sum_{x \neq 0} e_p \left(ux + v(A2^{d-1} x^d) \right)$$

$$= \frac{|I_3|^3 |I_4| (p-1)}{p^2} + \text{Error}.$$

We define

$$\Phi_d := \max_{(u,v)\neq(0,0)} \left| \sum_{x=1}^{p-1} e_p\left(ux + vx^d\right) \right|$$

Then $|\text{Error}| \leq \Phi_d |I_3|^{3/2} |I_4|^{1/2}$.

Theorem (Cochrane, P., Pinner)

If $(d, p-1) = 1$, $p \nmid A$, and $\Phi_d \leq \frac{p}{16}$ then $A\mathbb{E}^d \cap \mathbb{O}$ is nonempty.

Define $d_1 = (d-1, p-1)$. Previous work of Cochrane and Pinner gives for any nonzero a, b:

$$|\Phi_d - d_1| \leq \frac{p^{3/2}}{d_1}.$$

So

$$32\sqrt{p} < d_1 < \frac{p}{32} \text{ implies } \Phi_d < \frac{p}{16}.$$

Things go bad if $d_1 > p/16 + 16\sqrt{p}$ since $\Phi_d \approx d_1$ when $d_1 > p^{3/4}$.

$$S_+ := S_+(k,\ell) = \sum_{x=1}^{p-1} e_p(ax^k + bx^\ell), p \nmid ab, 1 \le \ell < k < p-1$$

$$S_- := S_-(k,\ell) = \sum_{x=1}^{p-1} e_p(ax^k + bx^{-\ell}), p \nmid ab, 1 \le \ell \le k, (k+\ell) < p-1$$

Theorem (Cochrane, P., Pinner)

For any integer d with $(d, p-1) = 1$, if $d_1 < .2(p-1)^{16/23}$ then $|S_\pm(k,\ell)| \le 10.811 p^{89/92}$.

This theorem says $\Phi_d < 10.811 p^{89/92}$ which is less than $p/16$ when $p > (10.811 \cdot 16)^{92/3} = 4.29 \cdot 10^{68}$.

Idea of this proof is to apply a transformation to $S_\pm$ sending x to x^m where m is chosen to satisfy the following:

- $mk \equiv \alpha \bmod (p-1)$
- $\pm m\ell \equiv \beta \bmod (p-1)$ ($\pm$ dependent on S_+ or S_-)
- $0 \leq \alpha \leq \frac{1}{c}(p-1)^{16/23}$, $|\beta| \leq c(p-1)^{7/23}$ where $c = 5.146$
- $(\alpha, \beta) \neq (0,0)$

We now have $S_\pm$ in terms of x^α and x^β and we use Mordell bounds and the following lemma to get improved bounds.

Set $\lambda = (\ell, k, p-1)$, $\lambda_1 = (\ell, k)$, $\ell_+ = \ell$, $\ell_- = 2\ell$

Lemma (Cochrane and Pinner, 2003)

For $k \leq \frac{1}{32}(p-1)^{\frac{2}{3}}\lambda_1^{\frac{1}{6}}\ell_\pm^{\frac{1}{6}}$,

$$|S_\pm| \leq p^{\frac{1}{4}}\left(\lambda^2(p-1)^2 + 2k^2\ell_\pm(p-1) + (p-1)^2 M\right)^{1/4}$$

where $M = \max\{758 \cdot 5^{2/3} k l_\pm \delta_\pm^{\frac{-1}{3}} \lambda/\lambda_1,\ 557\delta_\pm\lambda\}$ *and* $\delta_\pm = (k \mp \ell)/\lambda_1$

Multiplicative Character Approach

What if d_1 is large? (larger than $.2(p-1)^{16/23}$)

Theorem (Cochrane, P., Pinner)

(a) Let $d_1 = (d-1, p-1) < p-1$. *If* $d_1 > 8(\frac{4}{\pi^2}\log p + 1)^2\sqrt{p}$ *then* $A\mathbb{E}^d \cap \mathbb{O}$ *is nonempty.*
(b) If $p > 8.8 \cdot 10^7$ *and* $d_1 > 17\sqrt{p}$ *then* $A\mathbb{E}^d \cap \mathbb{O}$ *is nonempty.*

So $d_1 > .2(p-1)^{16/23} > 17\sqrt{p}$ when $p > 7.3 \cdot 10^9$.

- Let $k = (p-1)/d_1$
- Choose B such that $p \nmid B$ and $AB^{d-1} \not\equiv 1 \bmod p$
- Find $-p/2 < C < p/2$ such that $C \equiv AB^{d-1} \bmod p$

If there were some $Bz^k \in \mathbb{E}$ with $BCz^k \in \mathbb{O}$ then $A(Bz^k)^d \equiv BCz^k \bmod p$ (so $A\mathbb{E}^d \cap \mathbb{O}$ is nonempty).

Let $x \equiv Bz^k \bmod p$ and $y \equiv BCz^k \bmod p$.

We want to know when $y \equiv Cx \bmod p$ has a solution for $x \in \mathbb{E}$, $B^{-1}x$ a kth power, and $y \in \mathbb{O}$. Equivalently, we want to know when N is positive:

$$N = \frac{1}{k} \sum_{x \in \mathbb{E}} \left(\sum_{\psi^k = \psi_0} \psi(B^{-1}x) \right) \chi_{\mathbb{E}}(x) \chi_{\mathbb{O}}(Cx).$$

The End