Permutations of even residues modulo p

Jennifer Paulhus

Kansas State University
paulhus@math.ksu.edu

Decimations of l-sequences and permutations of even residues mod p

To appear.

joint work with

Jean Bourgain, Todd Cochrane, and Christopher Pinner

Available at: http://www.math.ksu.edu/$\sim$paulhus

The Problem

Given a prime p, pick integers d and A with $p \nmid A$, $(d, p-1) = 1$. Define $\mathbb{E} = \{2, 4, 6, \ldots, p-1\}$ and $\mathbb{O} = \{1, 3, 5, \ldots, p-2\}$ to be the even and odd residues mod p.

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).

The Problem

Given a prime p, pick integers d and A with $p \nmid A$, $(d, p-1) = 1$. Define $\mathbb{E} = \{2, 4, 6, \ldots, p-1\}$ and $\mathbb{O} = \{1, 3, 5, \ldots, p-2\}$ to be the even and odd residues mod p.

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).

There is the trivial case ($d = A = 1$).

The Problem

Given a prime p, pick integers d and A with $p \nmid A$, $(d, p-1) = 1$. Define $\mathbb{E} = \{2, 4, 6, \ldots, p-1\}$ and $\mathbb{O} = \{1, 3, 5, \ldots, p-2\}$ to be the even and odd residues mod p.

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).

There is the trivial case ($d = A = 1$). And there are some other cases. For instance if $p = 5$, $d = 3$, and $A = 3$, then the map sending x to Ax^d sends the residue 2 to the residue 4 and sends the residue 4 to the residue 2.

The following 6 cases give permutations of $\mathbb{E}$:

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

Conjecture (Goresky and Klapper, 1997)

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.

The following 6 cases give permutations of $\mathbb{E}$:

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

Conjecture (Goresky and Klapper, 1997)

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 (Bourgain, Cochrane, P., Pinner)

For $p > 2.26 \cdot 10^{55}$ and $(A, d) \neq (1,1)$, $A\mathbb{E}^d \cap \mathbb{O}$ is nonempty.

Motivation

Definition

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

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

Motivation

Definition

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

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

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

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

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

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 $\mathbf{a_t} = \{\mathrm{a}_{i+t}\}_i$.

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 (GK-Conjecture)

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

Conjecture (GK-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.

Conjecture (GK-Conjecture)

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

$\mathbf{a}$ 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 (GK-Conjecture)

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

$\mathbf{a}$ 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 (GK-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.

Previous Work

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. $0 < d \leq \frac{(p^2-1)^4}{2^{24}p^7}$ or $0 > d \geq -\frac{(p^2-1)^4}{2^{25}p^7}$

Our Result

Theorem (Bourgain, Cochrane, P., Pinner)

For $p > 2.26 \cdot 10^{55}$ *and* $(A, d) \neq (1, 1)$, $A\mathbb{E}^d \cap \mathbb{O}$ *is nonempty.*

Our Result

Theorem (Bourgain, Cochrane, P., Pinner)

For $p > 2.26 \cdot 10^{55}$ and $(A, d) \neq (1, 1)$, $A\mathbb{E}^d \cap \mathbb{O}$ is nonempty.

Goal: Find $x \in \mathbb{E}$ such that $Ax^d \in \mathbb{O}$.

Our Result

Theorem (Bourgain, Cochrane, P., Pinner)

For $p > 2.26 \cdot 10^{55}$ and $(A, d) \neq (1, 1)$, $A\mathbb{E}^d \cap \mathbb{O}$ is nonempty.

Goal: Find $x \in \mathbb{E}$ such that $Ax^d \in \mathbb{O}$.

Show there exists a solution (x, y) to the equation $A(2x)^d = 2y - 1$ over $\mathbb{Z}/p\mathbb{Z}$ with $(x, y) \in I_1 \times I_2$.

$I_1 = \left\{0, 1, 2, \ldots, \frac{p-1}{2}\right\} \in \mathbb{Z}/p\mathbb{Z} \qquad I_2 = I_1 - \{0\} \in \mathbb{Z}/p\mathbb{Z}$.

For the intervals $I = \{0, 1, 2, \ldots, \frac{p-1}{4}\}$ and $J = \{1, 2, \ldots, \frac{p+1}{4}\}$, we let χ_I and χ_J be their characteristic functions.

For the intervals $I = \{0, 1, 2, \ldots, \frac{p-1}{4}\}$ and $J = \{1, 2, \ldots, \frac{p+1}{4}\}$, we let χ_I and χ_J be their characteristic functions.

Given any two functions f and g on $\mathbb{Z}/p\mathbb{Z}$ we define the convolution as $f * g\ (x) = \sum_u f(u)g(x-u)$.

For the intervals $I = \{0, 1, 2, \ldots, \frac{p-1}{4}\}$ and $J = \{1, 2, \ldots, \frac{p+1}{4}\}$, we let χ_I and χ_J be their characteristic functions.

Given any two functions f and g on $\mathbb{Z}/p\mathbb{Z}$ we define the convolution as $f * g\ (x) = \sum_u f(u)g(x-u)$.

We then define $\alpha(x, y) = \chi_I * \chi_I\ (x) \cdot \chi_I * \chi_J\ (y)$.

α is supported on $I_1 \times I_2$ (since $I + I \subset I_1$ and $I + J \subset I_2$).

For the intervals $I = \{0, 1, 2, \dots, \frac{p-1}{4}\}$ and $J = \{1, 2, \dots, \frac{p+1}{4}\}$, we let χ_I and χ_J be their characteristic functions.

Given any two functions f and g on $\mathbb{Z}/p\mathbb{Z}$ we define the convolution as $f * g\ (x) = \sum_u f(u)g(x-u)$.

We then define $\alpha(x, y) = \chi_I * \chi_I\ (x) \cdot \chi_I * \chi_J\ (y)$.

α is supported on $I_1 \times I_2$ (since $I + I \subset I_1$ and $I + J \subset I_2$).

Goal: Show $\sum_{A(2x)^d = 2y-1} \alpha(x, y) > 0$.

By results in finite Fourier series,

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

where the $a(u, v)$ are the Fourier coefficients

By results in finite Fourier series,

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

where the $a(u,v)$ are the Fourier coefficients

We have a main term $a(0,0)(p-1) = \frac{p-1}{p^2}|I|^3|J|$.

We estimate the error term (using various techniques, in particular binomial exponential sum bounds) and get that the main term is greater than the error term when $M < .000823p^3$

$M = \#\{(x_1,x_2,x_3,x_4) \in (\mathbb{Z}/p\mathbb{Z}^*)^4 \mid x_1+x_2 = x_3+x_4, x_1^d+x_2^d = x_3^d+x_4^d\}$

Theorem (Bourgain, Cochrane, P., Pinner)

If $M < .000823p^3$, the GK-conjecture holds.

Theorem (Bourgain, Cochrane, P., Pinner)

If $M < .000823p^3$, the GK-conjecture holds.

Let $d_1 = (d-1, p-1)$. As long as d_1 is not too large we can bound M using previous results of Cochrane and Pinner. (Otherwise we have to do more work and actually get a better result!)

Theorem (Bourgain, Cochrane, P., Pinner)

If $M < .000823p^3$, the GK-conjecture holds.

Let $d_1 = (d-1, p-1)$. As long as d_1 is not too large we can bound M using previous results of Cochrane and Pinner. (Otherwise we have to do more work and actually get a better result!)

Theorem (Bourgain, Cochrane, P., Pinner)

For any integer d with $(d, p-1) = 1$ and $d_1 < .18(p-1)^{16/23}$ then $M \leq 13658p^{66/23}$.

This gives us the conjecture for $p > 2.26 \cdot 10^{55}$.

Large d_1

If d_1 is larger than $0.18(p-1)^{16/23}$ we use multiplicative characters to get the following.

Large d_1

If d_1 is larger than $0.18(p-1)^{16/23}$ we use multiplicative characters to get the following.

Theorem (Bourgain, 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 the GK-conjecture holds.*
(b) If $p > 2.1 \cdot 10^7$ *and* $d_1 > 10\sqrt{p}$ *then the GK-conjecture holds.*

Possible Generalizations

1. Apply the methods in the paper to q-ary l-sequences:
$a_i \equiv (q^{-i} \bmod p) \bmod q$ where q is a primitive root mod$p$.
(This would be the output of a feedback with carry shift register (FCSR) in which the cells and multipliers are in $\mathbb{Z}/q\mathbb{Z}$.)

Possible Generalizations

1. Apply the methods in the paper to q-ary l-sequences: $a_i \equiv (q^{-i} \bmod p) \bmod q$ where q is a primitive root mod$p$. (This would be the output of a feedback with carry shift register (FCSR) in which the cells and multipliers are in $\mathbb{Z}/q\mathbb{Z}$.)

2. A problem of D.H. Lehmer: Obtain an asymptotic formula for the number N_{-1} of even residues $x \bmod p$ such that $x^{-1} \bmod p$ is an odd residue. Kloosterman sum estimates give $N_{-1} \sim p/4$.

Possible Generalizations

1. Apply the methods in the paper to q-ary l-sequences:
$a_i \equiv (q^{-i} \bmod p) \bmod q$ where q is a primitive root mod$p$.
(This would be the output of a feedback with carry shift register (FCSR) in which the cells and multipliers are in $\mathbb{Z}/q\mathbb{Z}$.)

2. A problem of D.H. Lehmer: Obtain an asymptotic formula for the number N_{-1} of even residues $x \bmod p$ such that $x^{-1} \bmod p$ is an odd residue. Kloosterman sum estimates give $N_{-1} \sim p/4$.

Given d relatively prime to $p-1$ obtain an asymptotic formula for the number N_d of even residues $x \bmod p$ such that $x^d \bmod p$ is an odd residue. What we have done is establish that N_d is nonzero.

The End