A generalization of the Goresky-Klapper conjecture

by

CJ Richardson

B.S., Baker University, 2012

AN ABSTRACT OF A DISSERTATION

submitted in partial fulfillment of the
requirements for the degree

DOCTOR OF PHILOSOPHY

Department of Mathematics
College of Arts and Sciences

KANSAS STATE UNIVERSITY
Manhattan, Kansas

2018

Abstract

For a fixed integer $n \geq 2$, we show that a permutation of the least residues mod p of the form $f(x) = Ax^k \bmod p$ cannot map a residue class mod n to just one residue class mod n once p is sufficiently large, other than the maps $f(x) = \pm x \bmod p$ when n is even and $f(x) = \pm x$ or $\pm x^{(p+1)/2} \bmod p$ when n is odd. We also show that for fixed n the image of each residue class mod n contains every residue class mod n, except for a bounded number of maps for each p, namely those with $(k-1, p-1) > (p-1)/1.6n^4$ and A from a readily described set of size less than $1.6n^4$. For $n > 2$ we give $O(n^2)$ examples of $f(x)$ where the image of one of the residue classes mod n does miss at least one residue class mod n.

A generalization of the Goresky-Klapper conjecture

by

CJ Richardson

B.S., Baker University, 2012

A DISSERTATION

submitted in partial fulfillment of the
requirements for the degree

DOCTOR OF PHILOSOPHY

Department of Mathematics
College of Arts and Sciences

KANSAS STATE UNIVERSITY
Manhattan, Kansas

2018

Approved by:

Major Professor
Christopher Pinner

Copyright

Abstract

For a fixed integer $n \geq 2$, we show that a permutation of the least residues mod p of the form $f(x) = Ax^k$ mod p cannot map a residue class mod n to just one residue class mod n once p is sufficiently large, other than the maps $f(x) = \pm x$ mod p when n is even and $f(x) = \pm x$ or $\pm x^{(p+1)/2}$ mod p when n is odd. We also show that for fixed n the image of each residue class mod n contains every residue class mod n, except for a bounded number of maps for each p, namely those with $(k-1, p-1) > (p-1)/1.6n^4$ and A from a readily described set of size less than $1.6n^4$. For $n > 2$ we give $O(n^2)$ examples of $f(x)$ where the image of one of the residue classes mod n does miss at least one residue class mod n.

Contents

List of Tables

Acknowledgments

With Thanks:

Christopher Pinner

Todd Cochrane

Michael Mossinghoff

Badria Alsulmi

Vincent Pigno

Chapter 1

Introduction

1.1 The Goresky-Klapper Conjecture

For an odd prime p we let I denote the reduced residues mod p,

$$I = \{1, 2, \ldots, p-1\},$$

and A and k integers with

$$|A| < p/2, \quad p \nmid A, \quad 1 \leq k < p-1, \quad \gcd(k, p-1) = 1, \tag{1.1}$$

so that the map $f : I \to I$ given by

$$f(x) = Ax^k \bmod p,$$

is a permutation of I.

Goresky & Klapper [8] divided I into the even and odd residues

$$E = \{2, 4, \ldots, p-1\}, \quad O = \{1, 3, \cdots, p-2\},$$

and asked when f could also be a permutation of E (equivalently O). Originally the problem was phrased in terms of decimations of ℓ-sequences and was restricted to cases where 2 is a primitive root mod p, but this is the form that we are interested in here. Apart from the identity map $(p; A, k) = (p; 1, 1)$ they found six cases

$$(p; A, k) = (5; -2, 3), (7; 1, 5), (11; -2, 3), (11; 3, 7), (11; 5, 9), (13; 1, 5),$$

and conjectured that there were no more for $p > 13$. This was proved for sufficiently large p in [2] and in full in [6]. Since $x \mapsto p - x$ switches elements of E and O, this is the same as asking when $f(E) = O$ or $f(O) = E$ on replacing A by $-A$.

Somewhat related is a question of Lehmer [9], Problem F12, p.381 concerning the number of x mod p whose inverse, $f(x) = x^{-1}$ mod p, has opposite parity. Since k is defined mod $(p-1)$ it is sometimes useful to allow negative exponents, $|k| < (p-1)/2$. This problem was solved by Zhang [17] using Kloosterman sums; see also the generalizations by Alkan, Stan and Zaharescu [1], Lu and Yi [10][11], Shparlinski [13][12], Xi and Yi [15], and Yi and Zhang [16].

1.2 Different Generalizations of Goresky-Klapper

Thinking of the evens and odds as a mod 2 restriction we can ask a similar question for a general modulus n. Namely we can divide up I into the n congruence classes mod n

$$I_j = \{x \;:\; 1 \leq x \leq p-1,\ x \equiv j \bmod n\}, \quad j = 0, \ldots, n-1.$$

There are several different ways we can generalize the Goresky-Klapper Conjecture to n. Here we consider 5 possibilities:

(i) When is $f(I_j) = I_j$ for all $j = 0, \ldots, n-1$?

(iia) When is $f(I_0), \ldots, f(I_{n-1})$ a permutation of $I_0, \ldots, I_{n-1}$?

(iib) When is $f(I_j) = I_j$ for some j?

(iii) When is there a pair s, j with $f(I_s) \subseteq I_j$?

(iv) When is there a pair s, j with $f(I_s) \cap I_j = \emptyset$?

Notice that for $n = 2$ these are all the same problem, but for general n they can be quite different (indeed the I_j will not even have the same cardinality unless we restrict to $p \equiv 1 \bmod n$). Note that these requirements become successively weaker (and the claim that there are no such examples for large enough p a successively stronger statement) as we move from (i) to (iia) or (iib), to (iii), to (iv). If the map f randomly distributes the values mod n then we might expect to have $|f(I_s) \cap I_j| \sim p/n^2$ and so, for fixed n, no examples of (i) through (iv) once p is sufficiently large. To make sense here we should probably think of p growing with n, for example we need $p > n$ so that all the residue classes are non-empty, and if (iii) or (iv) do not hold we are demanding at least two or at least n values in each image of each residue class and so must have $p > 2n$ or $p > n^2$ for this to have any chance of being true. However, as shown in [3] for $n = 2$, if the parameter

$$d := \gcd(k-1, p-1)$$

is large we can't expect this equal distribution. Indeed when n is odd it is not hard to see that we will have infinitely many examples of (*iib*) in addition to the identity map. From these possible generalizations we get the following Examples and Theorems.

1.3 Type (iib) Examples

Proofs for the various examples in this section will be given in Chapter 5

Example 1.3.1. *Suppose that*

$$f(x) = \pm x^{(p+1)/2} \ mod\ p.$$

If n is odd and $J \equiv 2^{-1}p \ mod\ n$ then

$$f(I_J) = I_J.$$

If $p > 607$ and

$$p > 2.51(n \log n)^2 \tag{1.2}$$

then each $f(I_j)$, with $j \neq J$ when n is odd, hits exactly two residue classes, namely I_j and $I_{\bar{j}}$ where $\bar{j} \equiv p - j$ mod n.

A similar situation occurs for the map $f(x) = -x \bmod p$; if $p > n$ and n is even then the $f(I_j) = I_{\bar{j}}$ will be a derangement (i.e. a permutation fixing no element) of the I_j, while if n is odd this f will fix I_J and derange the remaining I_j. The bound (1.2) can be improved by Burgess [4].

1.4 Main Type (iii) Results

Notice that in these examples the value of d is unusually large, namely $d = (p-1)$ or $(p-1)/2$. If d is not large then in fact each residue class does receive its fair share of values:

Theorem 1.4.1. *For all s, j*

$$|f(I_s) \cap I_j| = \frac{p}{n^2} + O(d \log^2 p) + O(p^{89/92} \log^2 p).$$

In particular, if n is fixed and $d = o(p/log^2 p)$, then

$$|f(I_s) \cap I_j| \sim p/n^2.$$

This follows at once from the more numerically precise statement in Theorem 3.0.1 below. In fact, as we show in Theorem 4.0.1 below, if we avoid those few cases in Example 1.3.1, then even for large d we are able to show that there are most finitely many cases of (iii); that is the image of each residue class $f(I_j)$ hits at least two different residue classes mod n. Combining Theorems 3.0.1 and 4.0.1 gives the result for all d:

Theorem 1.4.2. *If n is even and $f(x) \neq \pm x$ mod p or if n is odd and $f(x) \neq \pm x$ or $\pm x^{(p+1)/2}$ mod p, then there are no s, j with $f(I_s) \subseteq I_j$ once*

$$p \geq e^{333} (n \log n)^{184/3} .$$

1.5 Type (iv) Examples

If we want a stronger statement avoiding cases of (iv) even when d is large, that is, prove that the image of every residue class mod n hits every residue class mod n, then we will need to exclude more examples for $n > 2$. For the linear maps, $k = 1$, the image of each residue class mod n will miss at least one residue class mod n when the coefficient A is sufficiently small, or of the form

$$A = \frac{tp - r}{s}, \qquad (rt, s) = 1, \tag{1.3}$$

for some integers r, s, t with $s \neq 0$, and r and s sufficiently small.

Example 1.5.1. *Suppose that $f(x) = Ax \bmod p$. If A is an integer satisfying* (1.1) *and either*

(a) $|A| < n$, *or*

(b) *A is of the form* (1.3) *with* $|r| + |s| + \gcd(n, s) - 2 < n$,

then for each i there is at least one j with $f(I_i) \cap I_j = \emptyset$.

If the restriction takes the form $B < n$ then in each case the number of missed residue classes j will be at least $n - B$.

We can do likewise for exponent $k = \frac{1}{2}(p+1)$, though we must halve the range of restriction.

Example 1.5.2. *Suppose that $f(x) = Ax^{(p+1)/2}$ mod p. If A satisfies (1.1) and*

(a) $2|A| < n$, or

(b) A is of the form (1.3) with $2(|r| + |s| + \gcd(n, s) - 2) < n$,

then for each i there is at least one j with $f(I_i) \cap I_j = \emptyset$.

If the restriction takes the form $B < n$ then in each case the number of missed residue classes j will be at least $n - B$.

The ranges in Example 1.5.2 can be extended to resemble the linear case if we just want there to be at least one residue class whose image does not contain all classes.

Example 1.5.3. *Suppose that $f(x) = Ax^{(p+1)/2}$ mod p and $2^\beta || n$. If A satisfies (1.1) and*

(a) $2^\beta \mid A$ and $|A| < n$ and $J :\equiv 2^{-1}p$ mod $n/\gcd(n, A)$, or

(b) $2^\beta \nmid A$ and $|A| + \gcd(n, A) < n$ and

$$J :\equiv \frac{1}{2}\left(\frac{A}{\gcd(A,n)} \pm 1\right)\left(\frac{A}{\gcd(A,n)}\right)^{-1} p \text{ mod } \frac{n}{\gcd(n,2A)},$$

then $f(I_J) \cap I_j = \emptyset$ *for at least one* j.

If A *satisfies* (1.1) *and is of the form* (1.3) *with*

(c) $2^\beta \mid r$ *with* $|r|+|s|+\gcd(n,s)-2 < n$, *and* $J :\equiv 2^{-1}p \ mod\ n/\gcd(n,r)$, *or*

(d) $2^\beta \nmid r$ *with* $|r|+|s|+\gcd(n,s)+\gcd(n,r)-2 < n$, *and*

$$J :\equiv \frac{1}{2}\left(\frac{r}{\gcd(r,n)} \pm 1\right)\left(\frac{r}{\gcd(r,n)}\right)^{-1} p \ mod\ \frac{n}{\gcd(n,2r)},$$

then $f(I_J) \cap I_j = \emptyset$ *for at least one* j.

If the restriction takes the form $B < n$ *then in each case the number of missed residue classes* j *will be at least* $n - B$.

1.6 Main Type (iv) Results

It is not hard to see that for each $n \geq 3$ the examples in Section 1.5 give us exactly $O(n^2)$ examples of $f(x)$ where the image of at least one residue class misses out least one residue class mod n. Note, the cases of small A can be thought of as taking $s = 1$. It seems reasonable to conjecture that, as long as we avoid exponents $k = 1$ and $(p+1)/2$ and coefficients with restrictions similar to those in Examples 1.5.1, 1.5.2 or 1.5.3 then $f(I_i)$ will hit all residue classes once p is sufficiently large. Indeed if we take the set of absolute least residues

$$\mathscr{C} := \{Ax^{k-1} \text{ mod } p \ : \ 1 \leq x \leq p-1\}$$

and $\mathscr{C}$ contains an element with $n \le |C| \le p/n$ then we will have only finitely many occurences of (iv). Note this always happens when $n = 2$, other than the maps $f(x) = \pm x$ or the $\pm x^{(p+1)/2}$ considered in Example 1.3.1. If $\mathscr{C}$ contains only elements $p/n < |C| < p/2$ then, prompted by the examples in Example 1.5.1, 1.5.2 and 1.5.3, we write C in the form

$$C = \pm \frac{(tp - r)}{s}, \quad s, t > 0, \ (s, t) = 1. \tag{1.4}$$

If $|r|$ is large relative to s then again the image of each residue class will hit every residue class.

Theorem 1.6.1. *If $\mathscr{C}$ contains an element C with $n \le |C| \le p/n$ or a C with*

$$C = \pm \frac{(tp - r)}{s}, \quad s, t > 0, \ (s, t) = 1, \ (n + 3)s \le |r| \le \frac{p}{n},$$

and

$$p \ge e^{333} \left(n \log n\right)^{184/3},$$

then $f(I_i) \cap I_j \ne \emptyset$ for all i, j.

By the box principle it is possible to write any C with $p/n < |C| < p/2$ in the form (1.4) with

$$1 \le t \le \lceil n/2 \rceil, \quad |r| < p/n, \ \ 2t \le s \le nt, \tag{1.5}$$

where s is the nearest integer to tp/C. In particular for fixed n there will be only finitely many values of C, namely

$$\mathscr{B} = \mathscr{B}_1 \cup \mathscr{B}_2, \quad \mathscr{B}_1 := \{C \ : \ |C| < n\},$$

and

$$\mathscr{B}_2 := \{C \ : \ |C| = (pt-r)/s \text{ with } 0 < t \leq \lceil n/2 \rceil, \ 2t \leq s \leq nt, \ |r| < (n+3)s\},$$

which do not give us Theorem 1.6.1. For $n \geq 3$ we have $|\mathscr{B}| < 1.6n^4$. Since the number of elements in $\mathscr{C}$ is $(p-1)/d$ and $A \in \mathscr{C}$ this tells us that for all but a finite number of k and A the image of every residue class will contain every residue class.

Corollary 1.6.2. *If $d \leq (p-1)/1.6n^4$ or $A \notin \mathscr{B}$, and $p \geq e^{333}\left(n \log n\right)^{184/3}$ then $f(I_i) \cap I_j \neq \emptyset$ for all i, j.*

The $1.6n^4$ can undoubtedly be improved; the only $d = (p-1)/t$ that we know have to be excluded have $t = 1$ or 2. This gives us potentially $O(n^8)$ occurrences of (iv) for a given p while Example 1.5.1 only tells us there must be $O(n^2)$, with computational evidence suggesting that this is probably right.

Here we have not attempted to make the bounds on the size of p optimal and they can certainly be improved; for example if we simply wanted $|f(I_s) \cap I_j| \geq 1$, rather than the asymptotic count in Theorem 1.4.1, using convolutions as employed in [2] instead of indicator functions would remove the $\log n$ terms.

For a given n we know that there are at most finitely many occurences of

(i) but of course our bounds are far too large to obtain a complete determination as was done for $n = 2$ in [6].

Chapter 2

Conjectures

Computations were performed for the primes $p < 10000$ and moduli $n = 3$ through 8.

Only a few cases were found where $Ax^k \bmod p$ permutates every residue class:

Example 2.0.1. *The only cases of (i), that is $f(I_j) = I_j$ for all j, found for $3 \leq n \leq 8$ and $p < 5000$, were $n = 3$, $(p; A, k) = (5; -1, 3)$ and $(7; -3, 5)$.*

For $n = 4$ and 5 examples of (iib) were found, that is where $f(I_1), \ldots, f(I_n)$ is a permutation of $I_1, \ldots, I_n$:

$$n = 4, \quad (p, A, k) = (11; \pm 1, 9), (13; \pm 2, 5)$$

$$n = 5, \quad (p; A, k) = (7, \pm 1, 5).$$

In Theorem 1.4.2 we showed the existence of a constant $K(n)$ such that for $p > K(n)$ and $f(x) \neq \pm x$ or $\pm x^{(p+1)/2} \bmod p$, every residue class is mapped to at least two different residue classes. The constant $K(n) = e^{333}\,(n\log n)^{184/3}$ obtained there is undoubtedly far from the truth. Table A gives the examples of $f(x) = Ax^k \bmod p$ with $f(I_i) \subseteq I_j$ for some i, j, found for $3 \leq n \leq 8$ and $2n < p < 1000$. Since Ax^k has this property if and only if $-Ax^k$ does, we just consider positive A. From this data we conjecture

Conjecture 2.0.1. *The optimal values for $K(n)$ for $n = 3$ through 8 are*

$$K(3) = 17, \quad K(4) = 13, \quad K(5) = 43, \quad K(6) = 17, \quad K(7) = 37, \quad K(8) = 43.$$

It is noticeable that our infinite families of examples of $f(x) = Ax^k \bmod p$ with $f(I_i) \cap I_j = \emptyset$ all have exponent $k = 1$ or $(p+1)/2$.

Checking the primes $p < 10,000$, examples of $f(x) = Ax^k \bmod p$ with $k \neq 1$, $(p+1)/2$ and $f(I_i) \cap I_j$ for some (i, j) typically only occurred for the small primes. The five largest examples found for each $n = 3$ to 8 are recorded in the Table A.2. Notice that if Ax^k has this property with $2j \equiv p \bmod n$ then so will $Ax^{k'}$ when $k' = k \pm (p-1)/2$ has $(k', p-1) = 1$; a number of these pairs can be seen in the table.

In view of this data it is tempting to make the following conjecture.

Conjecture 2.0.2. *For a given n there is $C(n)$ such that once $p > C(n)$ any $f(x) = Ax^k \bmod p$ with $k \neq 1, (p+1)/2$ has $f(I_i) \cap I_j \neq \emptyset$ for all i, j.*

For $n = 3$ through 8 the optimal $C(n)$ is

$$C(3) = 127, \quad C(4) = 271, \quad C(5) = 601, \quad C(6) = 571, \quad C(7) = 1733, \quad C(8) = 1777.$$

For $k = 1$ we know from Example 1.5.1 that there will be $f(x) = Ax$ mod p with $f(I_i) \cap I_j = \emptyset$ for some (i, j). These A for $n = 3$ to 8 are shown in Table A.3 (whenever p is in the correct congruence class to make that A an integer).

Similarly when $p \equiv 1$ mod 4 and $k = (p + 1)/2$ Examples 1.5.3 gives us $f(x) = Ax^{(p+1)/2}$ mod p with $f(I_i) \cap I_j = \emptyset$ for some (i, j). These A for $n = 3$ to 8 are shown in Table A.4.

Experimentation for $n = 3$ to 8 yielded for even n a few additional values of A producing type (iv) examples for Ax or $Ax^{(p+1)/2}$ (whenever p was in the residue class producing an integer A of that form). These are shown in Table A.5. Their form only just misses out inclusion in Examples 1.5.1 and 1.5.3 (corresponding to equality rather than strict inequality in the restriction on r and s). It is not hard to check that the proof of those examples (putting numerical values to gcds and integer parts) also applies to these A for those particular n.

After excluding the values of A in Tables A.3, A.4 and A.5, few additional type (iv) exceptions were found in a search of $p < 10000$ and $k = 1$ or $(p + 1)/2$; the largest four encountered for each n are shown in Table A.6. In view of this data it seems reasonable to speculate that for large enough p the only type (iv) will come from A of the general type encountered in Examples 1.5.1 and 1.5.3.

Conjecture 2.0.3. *Suppose that $f(x) = Ax$ or $Ax^{(p+1)/2}$ mod p where A*

satisfies (1.1) *but is not of the form*

$$|A| < n \quad \textit{or} \quad A = (pt + r)/s \quad \textit{with} \quad |r| + |s| \le n.$$

Then for a given n *there is a* $c(n)$ *such that* $f(I_i) \cap I_j \neq \emptyset$ *for all* i, j *once* $p > c(n)$, *with*

$$c(3) = 17, \;\; c(4) = 61, \;\; c(5) = 137, \;\; c(6) = 197, \;\; c(7) = 277, \;\; c(8) = 937.$$

Chapter 3

Small $d = gcd(k-1, p-1)$

In this section we will discuss the situation when the $gcd(k-1, p-1)$ is small. In this case the residue classes will be well distributed. Because of this we can avoid Type (iv) situations.

Theorem 3.0.1. *Suppose that $p > 607$. Then for any A and k satisfying (1.1), $2 \leq n < p$, and $0 \leq s, j \leq n-1$, we have*

$$|f(I_s) \cap I_j| = M + E$$

with

$$M = \frac{1}{p} \left\lfloor \frac{p-1+n-s}{n} \right\rfloor \cdot \left\lfloor \frac{p-1+n-j}{n} \right\rfloor,$$

less one when $(s, j) = (0, 0)$, and

$$|E| \leq (d + 1 + 2.293p^{89/92}) \left(\frac{4}{\pi^2} \log p + 0.381 \right)^2.$$

In particular, if $d < .006p^{89/92}$ *and* $p > e^{333}(n\log n)^{184/3}$ *we have* $f(I_s) \cap I_j \neq \emptyset$ *for any* s, j.

Proof. For convenience we add $x = 0$ to I and regard $f(x) = Ax^k \bmod p$ as a map $f : \mathbb{Z}_p \to \mathbb{Z}_p$. We define I_j^* to be the congruence classes containing an element in I_j for $j = 1, \ldots, n-1$, and I_0^* the classes containing 0 or an element of I_0. We write

$$N_{sj} = |f(I_s^*) \cap I_j^*|$$

so that $|f(I_s) \cap I_j| = N_{sj}$ for $(s, j) \neq (0, 0)$ and $|f(I_0) \cap I_0)| = N_{00} - 1$. That is, we want to show $N_{sj} > 0$ for $(s, j) \neq (0, 0)$ and $N_{00} > 1$, for p sufficiently large.

We write $\mathscr{I}_j(x)$ for the characteristic function for I_j^* so that

$$N_{sj} = \sum_{x \bmod p} \mathscr{I}_s(x)\mathscr{I}_j(Ax^k).$$

Since $\mathscr{I}_t(x)$ is a periodic function mod p we have a finite Fourier expansion

$$\mathscr{I}_t(x) = \sum_{u \bmod p} a_t(u)e_p(ux)$$

where we define $e_p(x)$ to $e^{\frac{2\pi i x}{p}}$ and, for $t = 0, \ldots, n-1$,

$$a_t(u) = \frac{1}{p}\sum_{y \bmod p} \mathscr{I}_t(y)e_p(-yu) = \frac{1}{p}\begin{cases} \left\lfloor \frac{p-1+n-t}{n} \right\rfloor, & \text{if } u = 0, \\ e_p(-tu)e^{-\frac{\pi i n u}{p}\left\lfloor \frac{p-1-t}{n} \right\rfloor} \frac{\sin(\pi n u \left\lfloor \frac{p-1+n-t}{n} \right\rfloor/p)}{\sin(\pi n u/p)}, & \text{if } u \neq 0. \end{cases}$$

Hence, separating into zero and non zero values of u and v, and observing that Ax^k is a permutation of $\mathbb{Z}_p$, we have

$$N_{sj} = \sum_{x=0}^{p-1}\sum_{u=0}^{p-1}\sum_{v=0}^{p-1} a_s(u)e_p(ux)a_j(v)e_p(vAx^k) = M + T_1 + T_2 + E,$$

where

$$M = pa_s(0)a_j(0) = \frac{1}{p}\left\lfloor \frac{p-1+n-s}{n} \right\rfloor \cdot \left\lfloor \frac{p-1+n-j}{n} \right\rfloor,$$

$$T_1 = a_j(0)\sum_{u=1}^{p-1} a_s(u) \sum_{x=0}^{p-1} e_p(ux) = 0,$$
$$T_2 = a_s(0)\sum_{v=1}^{p-1} a_j(v) \sum_{x=0}^{p-1} e_p(vAx^k) = a_s(0)\sum_{v=1}^{p-1} a_j(v)\sum_{x=0}^{p-1} e_p(vx) = 0,$$

and

$$E = \sum_{u=1}^{p-1}\sum_{v=1}^{p-1} a_s(u)a_j(v)\sum_{x=0}^{p-1} e_p(ux+vAx^k).$$

Now from [7, Theorem 1.3] we have

$$\left|\sum_{x=0}^{p-1} e_p(ux+vAx^k)\right| \le 1 + d + 2.292p^{89/92},$$

and from [5, Theorem 1], writing $n_j = [(p-1+n-j)/n] < p$ and observing that nx is a permutation of the x mod p,

$$\sum_{u=1}^{p-1}|a_j(u)| \le \frac{1}{p}\sum_{x=1}^{p-1}\frac{|\sin(\pi x n_j/p)|}{|\sin(\pi x/p)|}$$
$$\le \frac{4}{\pi^2}\log p + .38 + \frac{0.608}{p} + \frac{0.116}{p^3} < \frac{4}{\pi^2}\log p + .381$$

for $p > 607$. Note for small k an improvement can be made using the Weil bound [14] instead. Hence

$$|E| \le (d+1+2.293p^{89/92})\left(\sum_{u=1}^{p-1}|a_s(u)|\right)\left(\sum_{v=1}^{p-1}|a_j(v)|\right)$$
$$\le (d+1+2.293p^{89/92})\left(\frac{4}{\pi^2}\log p + .381\right)^2.$$

Writing $p \equiv w \bmod n$, $1 \le w < n$, we have for $(j,s) \ne (0,0)$

$$M \ge \frac{1}{p}\left\lfloor\frac{p}{n}\right\rfloor^2 = \frac{1}{p}\left(\frac{p-w}{n}\right)^2 \ge \frac{p}{n^2} - \frac{2w}{n^2} \ge \frac{p}{n^2} - \frac{1}{2}$$

and for $j = s = 0$

$$M - 1 = \frac{1}{p}\left(\left\lfloor\frac{p-1}{n}\right\rfloor + 1\right)^2 - 1 = \frac{1}{p}\left(\frac{p+n-w}{n}\right)^2 - 1 > \frac{p}{n^2} - 1,$$

while for $d \le 0.006p^{89/92}$ and $p > 10^{92}$ we have

$$E \le 2.299p^{89/92}\left(\frac{4}{\pi^2}\log p + 0.381\right)^2.$$

Hence writing $p = C(n\log n)^{184/3}$ we check that for $n \ge 3$ and $\log C > 333$

we have

$$\frac{p}{n^2} - 1 > 2.299p^{89/92}\left(\frac{4}{\pi^2}\log p + 0.381\right)^2,$$

and hence $|f(I_s) \cap I_j| > 0$.

$\square$

Chapter 4

Large $d = gcd(k-1, p-1)$

As we saw from the examples, when we have a large $gcd(k-1,p-1)$, Type (iv) examples can occur, but we show that even for large d, with the exception of $f(x) = \pm x \bmod p$ and $f(x) = \pm x^{\frac{p+1}{2}} \bmod p$ we can not have Type (ii) maps $f(I_i) \subseteq I_j$.

Theorem 4.0.1. *Suppose that $f(x) \neq \pm x \bmod p$ when n is even, and $f(x) \neq \pm x$ or $\pm x^{\frac{1}{2}(p+1)} \bmod p$ when n is odd.*

If $p \geq 9.7 \times 10^8$ and $d \geq 0.6np^{1/2}\log^2 p$ then $f(I_s) \cap (I \setminus I_j) \neq \phi$ for all j, s.

Proof. Plainly $f(x) = \pm x \bmod p$ maps I_s to I_s or to $I_{\overline{s}}$ where $\overline{s} \equiv p - s \bmod n$ so must be excluded. The $f(x) = \pm x^{(p+1)/2}$ are dealt with in Example 1.3.1, see (5.1) below. So suppose that $(A,k) \neq (\pm 1, 1)$ or $(\pm 1, \frac{1}{2}(p+1))$.

Observe that the set of absolute least residues

$$\mathscr{C} = \{Ax^{k-1} \bmod p \ : \ 1 \leq x \leq p-1\}$$

must contain at least one element $C \neq \pm 1$. To see this observe that $\mathscr{C}$ contains $(p-1)/d$ elements and hence more than two unless $d = (p-1)$ or $(p-1)/2$ and $k = 1$ or $\frac{1}{2}(p+1)$. In these cases $\mathscr{C}$ contains only A or $\pm A$ and we just need to avoid $A = \pm 1$. We need to prove that $f(I_j) \cap (I \setminus I_j) \neq \phi$. We shall suppose that our $C \equiv AB^{k-1} \bmod p$ satisfies $1 < C < (p-1)/2$; if all the potential C's are negative we replace A by $-A$ and j by the least residue of $p - j$. We let

$$L := (p-1)/d$$

and

$$\mathscr{U} = \{x \in I_s \ : \ \ Cx \bmod p \in I \setminus I_j, \ \ x \equiv Bz^L \bmod p \text{ for some } z\}.$$

Notice that if x is in $\mathscr{U}$ we have

$$Ax^k \equiv Cx(B^{-1}x)^{k-1} \equiv Cxz^{L(k-1)} = Cx(z^{p-1})^{(k-1)/d} \equiv Cx \bmod p$$

and we have an $f(x)$ in $f(I_s) \cap (I \setminus I_j)$. So we need to show that $|\mathscr{U}| > 0$.

Let $\hat{G}$ denote the set of Dirichlet (multiplicative) characters on $\mathbb{Z}_p^*$ with principal character χ_0 and recall that

$$\sum_{\chi \in \hat{G}, \chi^L = \chi_0} \chi(y) = \begin{cases} L, & y \text{ is an } L\text{th power mod } p, \\ 0, & y \text{ is not an } L\text{th power mod } p. \end{cases}$$

Hence, writing $\mathscr{I}_j^c(x)$ for the characteristic function for the complement of I_j,

$$L|\mathscr{U}| = \sum_{x \in \mathbb{Z}_p^*} \mathscr{I}_s(x)\mathscr{I}_j^c(Cx) \sum_{\chi \in \hat{G}, \chi^L = \chi_0} \chi(B^{-1}x).$$

Separating the principal character from the remaining $L-1$ characters with $\chi^L = \chi_0$

$$L|\mathscr{U}| = M + E,$$

where M is our 'main term'

$$M = \sum_{x \in \mathbb{Z}_p^*} \mathscr{I}_s(x)\mathscr{I}_j^c(Cx),$$

and E the 'error'

$$E = \sum_{\chi^L = \chi_0, \chi \neq \chi_0} \chi(B^{-1}) S(\chi),$$

with

$$S(\chi) = \sum_{x \in \mathbb{Z}_p} \chi(x)\mathscr{I}_s(x)\mathscr{I}_j^c(Cx).$$

Error Term. Taking the finite Fourier expansion for the intervals as in the proof of Theorem 3.0.1 we have

$$\mathscr{I}_s(x) = \sum_{y \in \mathbb{Z}_p} a_s(y) e_p(yx), \quad |a_s(y)| = \frac{1}{p} \begin{cases} \left\lfloor \frac{p-1+n-s}{n} \right\rfloor, & \text{if } y = 0, \\ \frac{|\sin(\pi N_s n y/p)|}{|\sin(\pi n y/p)|}, & \text{if } y \neq 0, \end{cases}$$

and

$$\mathscr{I}_s^c(x) = \sum_{y \in \mathbb{Z}_p} a_s^c(y) e_p(yx), \quad a_s^c(y) = \begin{cases} 1 - a_s(0), & \text{if } y = 0, \\ -a_s(y), & \text{if } y \neq 0. \end{cases}$$

Again, separating the terms with u or v zero, we have

$$S(\chi) = \sum_{x \in \mathbb{Z}_p} \chi(x) \sum_{u=0}^{p-1} a_s(u) e_p(ux) \sum_{v=0}^{p-1} a_j^c(v) e_p(vCx) = T_1 + E_1 + E_2 + E_3$$

where

$$\begin{aligned} T_1 &= a_s(0) a_j^c(0) \sum_{x \in \mathbb{Z}_p} \chi(x) = 0, \\ E_1 &= a_s(0) \sum_{v=1}^{p-1} a_j^c(v) \sum_{x=0}^{p-1} \chi(x) e_p(Cvx), \\ E_2 &= a_j^c(0) \sum_{u=1}^{p-1} a_s(u) \sum_{x=0}^{p-1} \chi(x) e_p(ux), \end{aligned}$$

and

$$E_3 = \sum_{u=1}^{p-1} \sum_{v=1}^{p-1} a_s(u) a_j^c(v) \sum_{x \in \mathbb{Z}_p} \chi(x) e_p((u + Cv)x).$$

Recalling that, for a non-principal character χ, the classic Gauss sums

$$G(\chi, A) = \sum_{x=0}^{p-1} \chi(x) e_p(Ax)$$

satisfy $|G(\chi, A)| = p^{1/2}$ if $p \nmid A$ and trivially $G(\chi, A) = 0$ if $p \nmid A$, and again invoking [5, Theorem 1], we have for $p > 607$

$$|E_1| \le \frac{1}{p}\left\lfloor \frac{p-1+n-s}{n} \right\rfloor \sum_{v=1}^{p-1} |a_j^c(v)| p^{1/2} \le \frac{1}{p}\left\lfloor \frac{p-1+n}{n} \right\rfloor \left(\frac{4}{\pi^2}\log p + 0.381\right) p^{1/2},$$

$$|E_2| \le \left(1 - \frac{1}{p}\left\lfloor \frac{p-1+n-j}{n} \right\rfloor\right) \sum_{v=1}^{p-1} |a_s(u)| p^{1/2} \le \left(1 - \frac{1}{p}\left\lfloor \frac{p}{n} \right\rfloor\right) \left(\frac{4}{\pi^2}\log p + 0.381\right) p^{1/2},$$

$$|E_3| \le \left(\sum_{u=1}^{p-1} |a_s(u)|\right) \left(\sum_{v=1}^{p-1} |a_j^c(v)|\right) p^{1/2} \le \left(\frac{4}{\pi^2}\log p + 0.381\right)^2 p^{1/2}.$$

Hence, for $p > 9.7 \times 10^8$,

$$\begin{aligned} |S(\chi)| &\le \left(1 + \frac{1}{p}\right)\left(\frac{4}{\pi^2}\log p + 0.381\right) p^{1/2} + \left(\frac{4}{\pi^2}\log p + 0.381\right)^2 p^{1/2} \\ &< 0.2\, p^{1/2} \log^2 p - 4, \end{aligned}$$

and

$$|E| < 0.2 L p^{1/2} \log^2 p - 4.$$

Main Term. We have

$$M = |I_s| - \sum_{x \in \mathbb{Z}_p^*} \mathscr{I}_s(x)\mathscr{I}_j(Cx) = \left\lfloor \frac{p-1+n-s}{n} \right\rfloor - M_{sj},$$

where

$$M_{sj} = |\{x \in I_s \ : \ Cx \bmod p \in I_j\}|.$$

So for a lower bound on M we need an upper bound on M_{sj}. Since for

$1 \le x < p$ we have $0 < Cx < Cp$ we have

$$M_{sj} = \sum_{u=0}^{C-1} |\{x \in I_s \ : \ up \le Cx < (u+1)p, \ \ Cx - up \in I_j\}|$$

Note, if $x \equiv s \bmod n$ then $Cx - up \equiv j \bmod n$ requires $u \equiv K := (Cs - j)p^{-1} \bmod n$. Observing that the number of elements in a particular residue class mod n in an interval of length B is at most $\lfloor B/n \rfloor + 1$ we have

$$\begin{aligned} M_{sj} = & \sum_{\substack{u=0 \\ u \equiv K \bmod n}}^{C-1} \left| \left\{ x \in I_s \ : \ \frac{up}{C} \le x < \frac{up}{C} + \frac{p}{C} \right\} \right| \\ & \le \left(\left\lfloor \frac{C}{n} \right\rfloor + 1 \right) \left(\left\lfloor \frac{p/C}{n} \right\rfloor + 1 \right). \end{aligned}$$

Plainly

$$\left(\left\lfloor \frac{C}{n} \right\rfloor + 1 \right) \left(\left\lfloor \frac{p/C}{n} \right\rfloor + 1 \right) \le \left(\frac{C}{n} + 1 \right) \left(\frac{p}{Cn} + 1 \right) = \frac{p}{n^2} + \frac{C}{n} + \frac{p}{Cn} + 1,$$

where for $p/2n \ge C \ge 2n$

$$\frac{p}{n^2} + \frac{C}{n} + \frac{p}{Cn} + 1 \le \frac{2p}{n^2} + 1,$$

and for $2n \ge C \ge n$ or $p/n \ge C \ge p/2n$

$$\frac{p}{n^2} + \frac{C}{n} + \frac{p}{Cn} + 1 \le \frac{2p}{n^2} + 3.$$

Since $2 \leq C < p/2$, for $C < n$ we have

$$\left(\left\lfloor \frac{C}{n} \right\rfloor + 1\right)\left(\left\lfloor \frac{p/C}{n} \right\rfloor + 1\right) \leq 1 \cdot \left(\frac{p}{Cn} + 1\right) \leq \frac{p}{2n} + 1,$$

and when $C > p/n$

$$\left(\left\lfloor \frac{C}{n} \right\rfloor + 1\right)\left(\left\lfloor \frac{p/C}{n} \right\rfloor + 1\right) \leq \left(\frac{C}{n} + 1\right) \cdot 1 < \frac{p}{2n} + 1.$$

Hence for $n \geq 3$ we have

$$M_{sj} \leq \frac{2p}{3n} + 3$$

and

$$M \geq \left\lfloor \frac{p}{n} \right\rfloor - M_{sj} > \frac{p}{n} - 1 - M_{sj} \geq \frac{p}{3n} - 4.$$

Hence if $p/3n \geq (0.2p^{3/2} \log^2 p)/d$ we have $|E| < M$ and $|\mathscr{U}| > 0$.

$\square$

If we have a suitable C then we can show that each residue class gets mapped to all the residue classes.

Theorem 4.0.2. *Suppose that $\mathscr{C}$ contains an integer C with $n \leq |C| \leq p/n$. If $p \geq 9.7 \times 10^8$ and $d \geq 0.8n^2p^{1/2} \log^2 p$ then $f(I_s) \cap I_j \neq \emptyset$ for all j, s.*

Proof of Theorem 1.6.1. We proceed as the proof of Theorem 4.0.1 but with I_j in place of $I \setminus I_j$, and show that $f(I_s) \cap I_j \neq \phi$ by showing $|\mathscr{U}| > 0$, where

$$\mathscr{U} = \{x \in I_s \ : \ \ Cx \bmod p \in I_j, \ \ x \equiv Bz^L \bmod p \text{ for some } z\}.$$

Similarly

$$L|\mathscr{U}| = M + E$$

where

$$M = \sum_{x\in\mathbb{Z}_p^*} \mathscr{I}_s(x)\mathscr{I}_j(Cx) = M_{sj}$$

and

$$E = \sum_{\chi^L=\chi_0,\chi\neq\chi_0} \chi(B^{-1}) \sum_{x\in\mathbb{Z}_p} \chi(x)\mathscr{I}_s(x)\mathscr{I}_j(Cx).$$

As before we obtain

$$|E| < 0.2Lp^{1/2}\log^2 p.$$

This time we need a lower bound on M_{sj}.

Suppose that we have $n \leq C \leq p/n$.

Note that for $p/2n < C \leq p/n$ we have

$$\left\lfloor \frac{p}{nC} \right\rfloor = 1 > \frac{p}{2nC},$$

and for $C \leq p/2n$

$$\left\lfloor \frac{p}{nC} \right\rfloor > \frac{p}{nC} - 1 \geq \frac{p}{2nC}.$$

Similarly, for $n \leq C < 2n$ we have

$$\left\lfloor \frac{C}{n} \right\rfloor = 1 > \frac{C}{2n},$$

and for $C \geq 2n$

$$\left\lfloor \frac{C}{n} \right\rfloor \geq \frac{C}{n} - 1 \geq \frac{C}{2n}.$$

Hence, observing that a general interval of length ℓ or an interval of the form $[0, \ell - 1]$, will contain at least $\lfloor \frac{\ell}{n} \rfloor$ complete sets of residues mod n, we have

$$\left| \left\{ x \in I_s \ : \ \frac{up}{C} \leq x < \frac{up}{C} + \frac{p}{C} \right\} \right| \geq \left\lfloor \frac{p}{nC} \right\rfloor > \frac{p}{2nC},$$

and

$$|\{0 \leq u \leq C - 1 \ : \ u \equiv K \bmod n\}| \geq \left\lfloor \frac{C}{n} \right\rfloor > \frac{C}{2n},$$

giving

$$M_{sj} > \frac{C}{2n} \cdot \frac{p}{2nC} = \frac{p}{4n^2}.$$

Hence, as long as we have

$$\frac{p}{4n^2} \geq 0.2 \frac{p^{3/2} \log^2 p}{d},$$

we have $|\mathscr{U}| > 0$ and $f(I_s) \cap I_j \neq \emptyset$.

$\square$

Theorem 4.0.3. *Suppose that $\mathscr{C}$ contains a C of the form*

$$C = \pm \frac{(tp - r)}{s}, \ \ s, t > 0, \ (s, t) = (r, t) = 1, \ (n + 3)s \leq |r| \leq \frac{p}{n}.$$

If $p \geq 9.7 \times 10^8$ and $d \geq 1.2 n^2 p^{1/2} \log^2 p$ then $f(I_i) \cap I_j \neq \emptyset$ for all i, j.

Proof. We proceed as in Theorem 4.0.2. To estimate M_{ij} we split the x into the different residue classes a mod s and observe that for $x = a + sy$ we have

$$Cx = x\left(\frac{tp-r}{s}\right) \equiv \frac{(tp-r)a}{s} - ry \bmod p.$$

Hence, writing $\frac{(tp-r)a}{s} \equiv \alpha(a) \bmod p$ with $0 \le \alpha(a) < p$, we have

$$M_{ij} = \sum_{a=0}^{s-1} \left| \left\{ 0 \le y \le \frac{(p-1-a)}{s} \ : \ ys + a \in I_i, \ \alpha(a) - ry \bmod p \in I_j \right\} \right| .$$

If $b := \gcd(n,s) = 1$ then the condition $ys + a \in I_i$ reduces to the mod n congruence $y \equiv \lambda(a) := (i-a)s^{-1} \bmod n$. If $b > 1$ then we are reduced to the s/b values

$$\mathscr{A} = \{a \ : \ 1 \le a \le s, \ a \equiv i \bmod b\}$$

and the condition $ys + a \in I_i$ becomes $y \equiv \lambda(a) := (s/b)^{-1}(i-a)/b \bmod n/b$, that is $y \equiv \lambda_v(a) \bmod n$, $v = 1, \ldots, b$ with $\lambda_v(a) = \lambda(a) + vn/b$.

Suppose first that $r > 0$. Now any y with

$$-\left(\left\lfloor \frac{r(p-1-a)}{sp} \right\rfloor - 1\right) p \le \alpha(a) - ry < 0$$

will have $0 < y \le (p-1-a)/s$ and hence

$$M_{ij} \ge \sum_{a \in \mathscr{A}} \sum_{v=1}^{b} \sum_{u=1}^{\lfloor \frac{r(p-1-a)}{sp} \rfloor - 1} M_{ij}(a,v,u)$$

where

$$M_{ij}(a,v,u) = |\{y \equiv \lambda_v(a) \bmod n/b, \ \ -up \le \alpha(a) - ry < -(u-1)p, \ \alpha(a) - ry \bmod p \in I_j\}|.$$

The condition $\alpha(a) - ry \bmod p \in I_j$ becomes $\alpha(a) - ry + up \equiv j \bmod n$ and $u \equiv \mu(a,v) := (j + r\lambda_v(a) - \alpha(a))p^{-1} \bmod n$.

Hence

$$M_{ij} \ge \sum_{a \in \mathscr{A}} \sum_{v=1}^{b} \sum_{\substack{u=1 \\ u \equiv \mu(a,v) \bmod n}}^{\lfloor \frac{r(p-1-a)}{sp} \rfloor - 1} \left| \left\{ y \equiv \lambda_v(a) \bmod n, \ \frac{(\alpha(a) + up)}{r} - \frac{p}{r} < y \le \frac{(\alpha(a) + up)}{r} \right\} \right|.$$

Since $p/r > n$ we are guaranteed at least one element $y \equiv \lambda_v(a) \bmod n$ in the interval of length p/r when $n < p/r < 2n$ and at least $\lfloor p/rn \rfloor > p/rn - 1$ when $p/r \ge 2n$ we have

$$\left| \left\{ y \equiv \lambda_v(a) \bmod n, \ \frac{(\alpha(a) + up)}{r} - \frac{p}{r} < y \le \frac{(\alpha(a) + up)}{r} \right\} \right| \ge \frac{p}{2rn}.$$

Similarly, with $(n+3)s \le r < p/n$,

$$\left\lfloor \frac{r(p-1-a)}{sp} \right\rfloor - 1 \ge \frac{r(p-s)}{sp} - 2 \ge \frac{r}{s} - 3 \ge n.$$

So we get at least one u in the sum satisfying $u \equiv \mu(a,v) \bmod n$ for $(n+3) \le r/s < (2n+3)$ and $\lfloor (r/s - 3)/n \rfloor > r/ns - 3/n - 1$ for $(2n+3) \le r/s$ and

$$\left| \left\{ 1 \le u \le \left\lfloor \frac{r(p-1-a)}{sp} \right\rfloor \ : \ u \equiv \mu(a,v) \bmod n \right\} \right| \ge \frac{r}{s(2n+3)}.$$

Hence

$$M_{ij} \geq \frac{s}{b} \cdot b \cdot \frac{r}{s(2n+3)} \cdot \frac{p}{2rn} = \frac{p}{2n(2n+3)},$$

and making this greater than $|E| < 0.2(p/d)\sqrt{p}\log^2 p$ ensures that $\mathscr{U} \neq \phi$.

Similarly for $r < 0$ we have $0 < y \leq (p-1-a)/s$ whenever

$$p < \alpha(a) + |r|y \leq \left\lfloor \frac{(p-1-a)|r|}{sp} \right\rfloor p$$

and with $\mu(a,v) \equiv (\alpha(a) + |r|\lambda_v(a) - j)p^{-1} \bmod n$ we have that M_{ij} is at least

$$\sum_{a \in \mathscr{A}} \sum_{v=1}^{b} \sum_{\substack{u=1 \\ u \equiv \mu(a,v) \bmod n}}^{\lfloor \frac{|r|(p-1-a)}{sp} \rfloor - 1} \left| \left\{ y \equiv \lambda_v(a) \bmod n,\ \frac{(up-\alpha(a))}{|r|} < y \leq \frac{(up-\alpha(a))}{|r|} + \frac{p}{|r|} \right\} \right|$$

and we get the same estimates as before.

□

Notice that in the proof of Theorem 4.0.2 and Theorem 4.0.3 we had to count the $x \in I_i$ with $Cx \in I_j$ but could equally have counted $x \in I_j$ with $C^{-1}x \in I_i$. Not surprisingly replacing C by C^{-1} does not help with the problem C, for example if C is small then we can write $C^{-1} = -(tp-1)/C$ where $t \equiv p^{-1} \bmod C$ has $|t| \leq C/2$, and if $C = (tp-r)/s$ where r, s and t are all small then we can write $C^{-1} = (t'p-s)/r$ where $t' \equiv sp^{-1} \bmod r$ has $|t'| \leq r/2$.

Proof of Theorems 1.4.2 and 1.6.1. Suppose that $p > e^{333}(n\log n)^{184/3}$. Then certainly $p > 6.7 \times 10^8$. If $d \leq 0.006p^{89/92}$ then Theorem 1.4.2 follows from Theorem 3.0.1, while if $d \geq 0.6np^{1/2}\log^2 p$ it follows from Theorem 4.0.1. If neither of these occurs then $0.6np^{1/2}\log^2 p > d > 0.006p^{89/92}$ and $p^{43/92}/\log^2 p < 100n$. But this does not occur for $p > e^{333}(n\log n)^{184/3}$.

For Theorem 1.6.1 we use Theorem 4.0.2 or Theorem 4.0.3 instead of Theorem 4.0.1. $\square$

Proof of Corollary 1.6.2. We suppose that $\frac{p}{n} < C < \frac{p}{2}$. We first show (1.5). For $h = 0, \ldots, N := \lceil n/2 \rceil$ we write

$$h\frac{p}{C} = m_h + \delta_h, \quad m_h \in \mathbb{Z}, \quad -\frac{1}{2} < \delta_h \leq \frac{1}{2}.$$

Note, since $2 < p/C < n$, the nearest integers m_h must be distinct. With $N+1$ values in $(-\frac{1}{2}, \frac{1}{2}]$ we must have a pair $0 \leq h_1 < h_2 \leq N$ with

$$|\delta_{h_1} - \delta_{h_2}| < \frac{1}{N} \leq \frac{2}{n}, \quad (h_2 - h_1)p - (m_2 - m_1)C = (\delta_{h_2} - \delta_{h_1})C,$$

and setting

$$t = h_2 - h_1, \quad s = m_2 - m_1, \quad r = (h_2 - h_1)p - (m_2 - m_1)C,$$

we have

$$C = \frac{tp - r}{s}, \quad 0 < t \leq n, \quad |r| = |C||\delta_{h_2} - \delta_{h_1}| < \frac{2|C|}{n} < \frac{p}{n},$$

and

$$s = \frac{tp}{C} - (\delta_{h_2} - \delta_{h_1}),$$

so that s is the nearest integer to tp/C and, since $2 < p/C < n$, satisfies $2t \leq s \leq nt$. We can assume $\gcd(s,t) = 1$; any common factor also divides r and we can divide through.

Counting the elements of $\mathscr{B}_2$ the number of t is at most $(n+1)/2$, and for a given t the number of s is at most $(n-2)t + 1$ and for given s and t the number of $|r| < (n+3)s$ with $r \equiv tp \bmod s$ is $2(n+3)$. Hence with the choice of sign we have

$$|\mathscr{B}_2| \leq 2 \cdot 2(n+3) \cdot \sum_{t=1}^{n} ((n-2)t+1) \leq \frac{1}{2}(n+3)(n+2)(n+1)(n-1)$$

and for $n \geq 3$

$$|\mathscr{B}| \leq \frac{1}{2}(n+3)(n+2)(n+1)(n-1) + 2n \sim \frac{1}{2}n^4,$$

with $|\mathscr{B}| \leq \frac{14}{9}n^4$ for $n \geq 3$, and $|\mathscr{B}| < n^4$ for $n \geq 6$. $\square$

Chapter 5

Proof of Examples

Proof of Example 1. Suppose that $f(x) = \pm x^{(p+1)/2} \bmod p$. We have

$$x^{(p+1)/2} = x \cdot x^{(p-1)/2} \equiv x \left(\frac{x}{p}\right) \equiv \pm x \bmod p,$$

and $f(x) = x$ or $p - x$, where $(p-x) \equiv x \bmod n$ exactly when $x \equiv 2^{-1}p \bmod n$ if n is odd and in no cases if n is even, and the first claim is plain.

If n is even, or n is odd and $j \neq J$, then $x \not\equiv p - x \bmod n$ for x in I_j, and $f(I_j)$ will hit two different residue classes as long as I_j contains both quadratic residues and non-residues. Hence, we just need to show that

$$\mathscr{U}_1 = \left\{ x \in I_j \ : \ \left(\frac{x}{p}\right) = 1 \right\}, \quad \mathscr{U}_{-1} = \left\{ x \in I_j \ : \ \left(\frac{x}{p}\right) = -1 \right\},$$

are both non-empty. We have, for $\delta = \pm 1$,

$$|\mathscr{U}_\delta| = \frac{1}{2} \sum_{x \in I_j} \left(1 + \delta \left(\frac{x}{p} \right) \right) = \frac{1}{2} \left(M + \delta E \right),$$

where

$$M = \sum_{x \in I_j} 1 = \left\lfloor \frac{p - 1 + n - j}{n} \right\rfloor \geq \frac{p}{n} - 1,$$

and, since $\sum_{x=1}^{p-1} \left(\frac{x}{p} \right) = 0$,

$$E = \sum_{x=1}^{p-1} \mathscr{I}_j(x) \left(\frac{x}{p} \right) = \sum_{x=1}^{p-1} \sum_{u=0}^{p-1} a_j(u) e_p(ux) \left(\frac{x}{p} \right) = \sum_{u=1}^{p-1} a_j(u) \sum_{x=1}^{p-1} e_p(ux) \left(\frac{x}{p} \right).$$

Hence, using the Gauss sum bound and [5, Theorem 1] as above,

$$|E| \leq \sum_{u=1}^{p-1} |a_j(u)| \sqrt{p} \leq \left(\frac{4}{\pi^2} \log p + 0.381 \right) \sqrt{p} < 0.5 \sqrt{p} \log p - 1,$$

for $p > 607$, and if $p/n \geq 0.5\sqrt{p} \log p$ we are guaranteed that $|\mathscr{U}_1|$ and $|\mathscr{U}_{-1}|$ are both non-empty. Note that we have $\sqrt{p}/\log p > 0.5n$ when $p \geq 2.51(n \log n)^2$. It certainly holds when

$$d = \frac{1}{2}(p - 1) \geq 0.25 n \sqrt{p} \log p, \tag{5.1}$$

weaker than the assumption made in Theorem 4.0.1.

□

Proof of Example 1.5.1. (a) Suppose $A > 0$ then each Ax, $x = 1, .., p-1$ will lie in $[1, A(p-1)]$ with $A(p-1) < Ap$. So reducing to lie in $[1, p)$ we have

$$Ax \bmod p = Ax - jp, \ \ 0 \le j \le A - 1.$$

For x in I_i we have $Ax - jp \equiv Ai - jp \bmod n$ with at most A different values of j, and $Ax \bmod p$ can take at most A different values mod n. Similarly the $-Ax \bmod p$ take the form $p - (Ax - jp) = (j+1)p - Ax$, $0 \le j < A$, giving at most A classes mod n. Therefore $f(x) = Ax \bmod p$ or $-Ax \bmod p$ with $A < n$ must omit at least $n - A$ classes.

(b) Suppose that $A = (tp - r)/s$ with $s > 0$ and $1 \le x < p$. We divide x into the various residue classes mod s. Since $\gcd(s, t) = 1$ we write

$$x \equiv t^{-1}a \bmod s, \ \ 1 \le a \le s.$$

Then

$$Ax \equiv \frac{(ap - rx)}{s} \bmod p.$$

Suppose first that $r > 0$, and set

$$r = hs + r_0, \ 1 \le r_0 < s.$$

We have

$$\frac{(ap - rx)}{s} < \frac{ap}{s} \le p,$$

and

$$\frac{(ap - rx)}{s} > \frac{(ap - rp)}{s} = \left(-h + \frac{a - r_0}{s}\right) p.$$

Hence the least residue of Ax mod p is

$$\frac{(ap - rx)}{s} + jp$$

where j is one of the $h+1$ possibilities $0, 1, \ldots, h$ if $a \geq r_0$, or the $h+2$ possibilities $0, 1, \ldots h, h+1$ for $1 \leq a \leq r_0 - 1$.

Therefore, writing $m = js + a$, we have $1 \leq m \leq (h+1)s + (r_0 - 1) = r + s - 1$ and the least residues take the form

$$\frac{mp - rx}{s}, \quad 1 \leq m \leq r + s - 1, \quad m \equiv tx \bmod s.$$

Let $b = gcd(n, s)$ and suppose that x is in I_i. If $b = 1$ then, for each m, we have

$$(mp - rx)/s \equiv (mp - ri)s^{-1} \bmod n$$

and hence at most $r + s - 1$ residue classes mod n. If $b > 1$ then $m \equiv ti$ mod b and, for a given m, plainly $(mp - rx)/b \equiv (mp - ri)/b$ mod n/b giving

$$(mp - rx)/s \equiv (s/b)^{-1}(mp - ri)/b \bmod n/b.$$

So we will have b possible residue classes mod n for each of the m in $1 \leq m \leq r + s - 1$ lying in a particular residue class $m \equiv ti$ mod b. That is, at most

$$b\left\lceil \frac{r + s - 1}{b} \right\rceil \leq b\left(\frac{r + s - 2}{b} + 1\right) = r + s + b - 2$$

residue classes mod n. So at least one residue class missed when this is less than n.

For $-Ax$ mod p our residue classes take the form

$$p - \left(\frac{mp - rx}{s} \right)$$

and the count is the same. This deals with $A = (tp + r)/s$ with $r, s > 0$.

$\square$

Proof of Example 1.5.2. Recall that $Ax^{(p+1)/2} \equiv \pm Ax \bmod p$. Counting the residue classes for Ax or $-Ax$ mod p gives at worst twice the total obtained in the proof of Example 1.5.1 for each of these, and a missed residue class when this is less than n.

$\square$

Proof of Example 1.5.3. (a) Suppose that $A > 0$. Notice that when n is odd or n is even and $2^\beta \mid A$ and $x \equiv 2^{-1}p \bmod n/(A, n)$ we have

$$Ax - jp \equiv (A - j)p - Ax \bmod n, \quad j = 0, \ldots, A - 1.$$

Thus, matching up the oppposite ends Ax and $Ap - Ax$, we can perfectly pair the residue classes $Ax, Ax - p, ..., Ax - (A - 1)p$ for Ax mod p and the classes $p - Ax, 2p - Ax, ..., Ap - Ax$ for $-Ax$ mod p in reverse order. Hence $Ax^{(p+1)/2}$ or $-Ax^{(p+1)/2} \equiv \pm Ax \bmod p$ can take at most A different values mod n when x is in I_J for any of the (n, A) values of J with $J \equiv 2^{-1}p$ mod $n/(A, n)$.

(b) If $2^\beta \nmid A$ then we can no longer match the end values and the best we can hope for is to match up (A,n) steps in. That is

$$Ax - (A,n)p \equiv Ap - Ax \bmod n,$$

so that the remaining $Ax-((A,n)+j)p$ match up with the $(A-j)p-Ax$ mod n. Thus we will just have the $Ax - jp$ with $0 \le j < (A,n)$ unmatched, and hence a total of $A+(A,n)$ residue classes. This requires $2Ax \equiv (A+(A,n))p$ mod n, that is $2A/(A,n)\ x \equiv (A/(A,n)+1)p$ mod $n/(A,n)$, equivalently $x \equiv \frac{1}{2}(A/(A,n)+1)p(A/(A,n))^{-1}$ mod $n/2(A,n)$. Similarly we could match at the other end $p - Ax \equiv Ax - (A-1-(A,n))p$ mod n for the same count.

(c) Suppose that n is odd or $2^\beta \mid r$ and that J satisfies $2J \equiv p$ mod $n/(n,r)$.

As in the proof of Example 1.5.1, for $A = (tp-r)/s$, $r, s > 0$ the classes for Ax mod p and $-Ax$ mod p with x in I_J will take the form

$$\left(\frac{mp-rx}{s}\right) \text{ and } p - \left(\frac{mp-rx}{s}\right)$$

respectively, with $1 \le m \le r+s-1$, and $m \equiv tx$ mod s. Writing $m' = r+s-m$ we have

$$p - \left(\frac{m'p - rx'}{s}\right) = \frac{(mp-rx)}{s} + \frac{r(x+x'-p)}{s}$$

where plainly $1 \le m \le r+s-1$ iff $1 \le m' \le r+s-1$ and, since $r \equiv pt$ mod s,

$$m' \equiv tx' \bmod s \quad \text{iff} \quad x' \equiv p - mt^{-1} \bmod s.$$

Note that when $b > 1$, the conditions $x \equiv mt^{-1} \bmod s$ with x in I_J and $m' \equiv tx' \bmod s$, x' in I_J both imply that $m \equiv tJ \bmod b$, since $J \equiv p - J \bmod b$.

If $b = 1$ then the x, x' in I_J have $x + x' - p \equiv 2J - p \equiv 0 \bmod n/(n, r)$ and

$$p - \left(\frac{m'p - rx'}{s}\right) \equiv \frac{(mp - rx)}{s} \equiv (mp - rJ)s^{-1} \bmod n$$

with the different m only giving us $r + s - 1$ different residue classes mod n.

Now suppose that $b > 1$ and x, x' are in I_J, and that we have an m with $1 \le m \le r + s - 1$ and $m \equiv tJ \bmod b$. Consider the x with

$$x \equiv J \bmod n/(n, r), \quad x \equiv mt^{-1} \bmod s.$$

If x_0 is one solution then the other x will satisfy $x \equiv x_0 \bmod ns/b(r, n)$. That is we will have b solutions mod $ns/(r, n)$

$$x = x_0 + \lambda ns/b(r, n) \bmod ns/(r, n), \quad 0 \le \lambda < b.$$

Similarly the

$$x' \equiv J \bmod n/(r, n), \quad x' \equiv p - mt^{-1} \bmod s$$

will have b solutions mod $ns/(r, n)$, namely, since $p - J \equiv J \bmod n/(n, r)$,

$$x' = p - x_0 - \lambda ns/b(r, n) \bmod ns/(r, n), \quad 0 \le \lambda < b.$$

Thus pairing up the x and x' with the same λ we get $r(x+x'-p) \equiv 0 \bmod ns$ and

$$p - \left(\frac{m'p - rx'}{s}\right) \equiv \frac{(mp - rx)}{s} \bmod n$$

perfectly pairing up the classes for $-Ax'$ and Ax. Counting the b values of λ for each m with $1 \leq m \leq r+s-1$ and $m \equiv tJ \bmod b$ gives the count as before.

(d) Suppose that n is odd or $2^\beta \nmid r$ and that J satisfies

$$2J \equiv \left(1 + \frac{r}{(r,n)}\right) p \left(\frac{r}{(r,n)}\right)^{-1} \bmod \frac{n}{(r,n)}$$

(the case with the minus sign is similar). Take $m' = r + s + (r,n) - m$ and write

$$p - \left(\frac{m'p - rx'}{s}\right) = \frac{mp - rx}{s} + \frac{r(x + x' - p) - (n,r)p}{s}.$$

with $1 \leq m' \leq r+s-1$, and hence $1 + (r,n) \leq m \leq r + s + (r,n) - 1$, and

$$x' \equiv m't^{-1} \equiv (r + (r,n))t^{-1} - mt^{-1} \bmod s.$$

Notice that if x' is in I_J then $m = s + r + (r,n) - m' \equiv r + (r,n) - tJ \equiv tJ \bmod b$, since $2Jt \equiv pt(r/(r,n))^{-1}(1 + r/(r,n)) \equiv ((r,n) + r) \bmod b$.

Suppose that x, x' are in I_J. If $(s,n) = 1$ then

$$r(x + x' - p) - (n,r)p \equiv (n,r)\left(2J\frac{r}{(r,n)} - p\left(\frac{r}{(r,n)} + 1\right)\right) \equiv 0 \bmod n$$

and

$$p - \left(\frac{m'p - rx'}{s} \right) \equiv \frac{mp - rx}{s} \equiv (mp - rJ)s^{-1} \bmod n.$$

For the $-Ax'$ mod p we need the $1 + (r, n) \leq m \leq r + s - 1 + (r, n)$ and for Ax mod p the $1 \leq m \leq r + s - 1$. Hence we have $1 \leq m \leq r + s + (r, n) - 1$ and at most $r + s + (r, n) - 1$ residue classes mod n.

Suppose that $b > 1$ and $m \equiv tJ \bmod b$, then taking x_0 to be a solution to

$$x \equiv J \bmod n/(n, r), \quad x \equiv mt^{-1} \bmod s,$$

the solutions take the form

$$x \equiv x_0 + \lambda ns/(r, n)b \bmod ns/(r, n), \quad 0 \leq \lambda < b.$$

Likewise, since $(r/(r, n))^{-1}(1 + r/(r, n))p - J \equiv J \bmod n/(r, n)$, the solutions to

$$x' \equiv J \bmod n/(n, r), \quad x' \equiv (r + (r, n))t^{-1} - mt^{-1} \bmod s$$

can be written

$$x' \equiv (r/(r, n))^{-1}(1 + r/(r, n))p - x_0 - \lambda ns/(r, n)b \bmod ns/(r, n), \quad 0 \leq \lambda < b,$$

where here we take $(r/(r, n))^{-1}$ to be an inverse of $r/(r, n)$ mod $ns/(r, n)$.

Pairing up the x and x' with the same λ we have

$$p - \left(\frac{m'p - rx'}{s} \right) \equiv \frac{mp - rx}{s} \equiv \frac{mp - rx_0}{s} - \lambda \frac{r}{(r, n)} \frac{n}{b} \bmod n.$$

With b choices of λ for each $m \equiv tJ \bmod b$ with $1 \leq m \leq r+s+(r,n)-1$ we have at most

$$b\left\lceil \frac{r+s+(r,n)-1}{b} \right\rceil \leq b\left(\frac{r+s+(r,n)-2}{b}+1\right) = r+s+(r,n)+(s,n)-2$$

residue classes mod n.

$\square$

Bibliography

[1] E. Alkan, F. Stan, and A. Zaharescu, *Lehmer k-tuples*, Proc. Amer. Math. Soc. **134** (2006), 2807–2818.

[2] J. Bourgain, T. Cochrane, J. Paulhus, and C. Pinner, *Decimations of l-sequences and permutations of even residues mod p*, SIAM J. Discrete Math. **23** (2009), 842–857.

[3] ———, *On the parity of kth powers mod p a generalization of a problem of Lehmer*, Acta Arith. **147** (2011), 173–203.

[4] D.A. Burgess, *A note on the distribution of residues and non-residues*, J. London Math. Soc. **38** (1963), 253–256.

[5] T. Cochrane, *On a trigonometric inequality of Vinogradov*, J. Number Theory **26** (1987), 9–16.

[6] T. Cochrane and S. Konyagin, *Proof of the Goresky Klapper conjecture on decimations of l-sequences*, SIAM J. Discrete Math. **25** (2011), 1812–1831.

[7] T. Cochrane and C. Pinner, *Explicit bounds on monomial and binomial exponential sums*, Q. J. Math. **66** (2017), 203–219.

[8] M. Goresky and A. Klapper, *Arithmetic cross-correlations of FCSR sequences*, IEEE Trans. Inform. Theory **43** (1997), 342–1346.

[9] R. K. Guy, *Unsolved problems in number theory*, 3 ed., Springer-Verlag, 2004.

[10] Y. Lu and Y. Yi, *On the generalization of the D. H. Lehmer problem*, Acta Math. Sin. **25** (2009), 1269–1274.

[11] ______, *On the generalization of the D. H. Lehmer problem ii*, Acta Math. Sin. **142** (2009), 179–186.

[12] I. Shparlinski, *On a generalisation of a Lehmer problem for arbitrary powers*, East-West J Math. **Special Vol.** (2008), 197–204.

[13] ______, *On a generalisation of a Lehmer problem*, Math. Z. **263** (2009), 619–631.

[14] A. Weil, *On some exponential sums*, Proc. Natl. Acad. Sci USA **34** (1948), 204–206.

[15] P. Xi and Y. Yi, *Generalized D. H. Lehmer problem over short intervals*, Glasg. Math. J. **53** (2011), 293–299.

[16] Y. Yi and W. Zhang, *On the generalization of a problem of D. H. Lehmer*, Kyushu J. Math. **56** (2002), 235–241.

[17] W. Zhang, *On a problem of D. H. Lehmer and its generalization*, Compositio Math. **86** (1993), 307–316.

Appendix A

Appendix: Tables

Data obtained through Microsoft Visual Studio and in collaboration with Mike Mossinghoff.

Table A.1: *Cases of $f(x) = Ax^k$ mod p with $f(I_i) \subseteq I_j$ for some i, j, for $3 \leq n \leq 8$, $2n < p < 1000$, excluding $f(x) = x$ or $x^{(p+1)/2}$.*

$n = 3$			
p	A	k	i
7	3	5	1,2,3
11	4	9	1
13	3	5	2
13	3	11	2
17	4	5	1
17	4	13	1

$n=4$			
p	A	k	i
11	1	9	1,2,3,4
13	2	5	1,2,3,4

$n=5$			
p	A	k	i
11	5	3	3
11	4	7	3
11	2	9	3
11	3	9	2,4
11	5	9	1,5
13	3	5	3,4,5
13	5	5	3,5
13	4	7	3,5
13	5	7	3,5
13	1	11	1,2
13	2	11	3,5
13	3	11	4
17	3	5	3,4
17	6	7	1
17	6	15	1
17	7	13	2,5
19	5	17	2
23	10	21	4
29	14	13	4,5
31	1	11	3
43	6	29	4

$n = 6$			
p	A	k	i
13	1	5	3,4
13	1	7	3,4,5
13	1	11	3,4
13	1	7	2
13	3	5	2,5
13	3	11	2,5
13	6	11	1,6
17	1	9	5,6
17	2	5	2,3
17	4	7	5,6
17	4	15	0,5,6
17	8	13	1,4

$n=7$			
p	A	k	i
17	1	7	1,2
17	1	15	1,2
17	2	3	5
17	2	11	5
17	3	5	3,7
17	3	13	3,7
17	4	5	5
17	4	7	0,3,7
17	4	13	5
17	4	15	3,7
17	5	3	3,7
17	5	11	3,7
17	6	3	3,7
17	6	11	3,7
17	7	5	3,7
17	7	13	3,7
17	7	15	4,6
17	8	7	5
17	8	15	5
19	2	17	6
19	3	7	5,7
19	3	11	6
19	3	17	0,5,7
19	5	5	6
19	6	7	5,7
19	6	11	5,7
19	7	11	5,7
19	7	7	6
19	8	13	6
23	8	21	1
23	9	21	3,6
29	14	13	4
29	14	27	4
31	2	29	5
37	16	17	4,5

$n = 8$			
p	A	k	i
17	3	3	1,8
17	5	3	3,6
17	7	3	2,7
17	5	5	3,6
17	6	5	1,8
17	8	5	4,5
17	1	7	3,6
17	8	7	1,8
17	1	9	0,1,3,6,8
17	3	11	1,8
17	5	11	3,6
17	6	11	1,4,5
17	2	13	2,7
17	5	13	3 ,6
17	6	13	8
17	1	15	3,6
17	3	15	3,4,5,7
17	8	15	1,8
19	1	5	3,8
19	3	5	4,7
19	6	5	5,6
19	3	7	3,8
19	5	7	4,5,6,7
19	1	11	4,7
19	2	11	5,6
19	9	11	3,8
19	4	13	5,6
19	9	13	3,4,7,8
19	1	17	1,2
19	5	17	3,8
19	8	17	5,6
19	9	17	4,7
23	2	3	7,8
23	3	5	7,8
23	10	5	7,8
23	6	17	7,8
23	11	17	7,8
23	1	19	7,8
23	10	21	7,8
29	1	15	2,3
29	7	19	6,7
31	5	11	3,4
41	1	21	3,6
43	2	13	3,8

Table A.2: *5 Largest $p < 10000$ with an $f(x) = Ax^k$ mod p, $k \neq 1$, $\frac{1}{2}(p+1)$ having $f(I_i) \cap I_j = \phi$ for some (i,j).*

	p	A	k	(i,j)
$n=3$	83	21,26	81	(1,1)
	89	17,21	23,67	(1,1)
	97	17	47,95	(2,2)
	109	44	53,107	(2,2)
	127	45,53	71	(2,2)
$n=4$	151	2	13	(1,4),(2,3)
	151	46	127	(3,1),(4,2)
	157	64	155	(2,2),(3,3)
	167	83	165	(1,1),(2,2)
	193	16,48	95	(2,2),(3,3)
	193	49	95	(2,3),(3,2)
	271	107	269	(1,1),(2,2)
$n=5$	479	142	477	(2,2)
	503	25	65	(4,4)
	503	243	363	(4,4)
	521	215	259,519	(3,3)
	541	176	269,539	(3,3)
	601	59	251,551	(3,3)
$n=6$	449	158	447	(5,5),(6,6)
	457	137	151	(3,3),(4,4)
	457	162	227	(1,1),(6,6)
	457	80,137	455	(3,3),(4,4)
	479	214	477	(5,5),(6,6)
	547	30	155	(3,3),(4,4)
	571	118	341	(3,3),(4,4)
$n=7$	1303	347	1301	(4,4)
	1321	232	329,989	(6,6)
	1409	416	703,1407	(1,1)
	1489	653	371,1115	(6,6)
	1733	670	865,1731	(2,2)
$n=8$	1249	36	623	(1,1),(8,8)
	1301	432	599	(5,5),(8,8)
	1381	648	1379	(5,8),(8,5)
	1637	437	1635	(6,7),(7,6)
	1777	176	1775	(3,6),(6,3)

Table A.3: *Type (iv) examples Ax mod p from Example 1.5.1*

n	A
3	$1, 2, (p-1)/2$
4	$1, 2, 3, (p-1)/2, (p \pm 1)/3$
5	$1, 2, 3, 4, (p-1)/2, (p-3)/2, (p \pm 1)/3, (p \pm 2)/3, (p \pm 1)/4$
6	$1, 2, 3, 4, 5, (p-1)/2, (p-3)/2, (p \pm 1)/3, (p \pm 1)/4, (p \pm 1)/5, (2p \pm 1)/5$
7	$1, 2, 3, 4, 5, 6, (p-1)/2, (p-3)/2, (p-5)/2, (p \pm 1)/3, (p \pm 2)/3, (p \pm 4)/3, (p \pm 1)/4, (p \pm 3)/4, (p \pm 1)/5, (p \pm 2)/5, (2p \pm 1)/5, 2(p \pm 1)/5, (p \pm 1)/6$
8	$1, 2, 3, 4, 5, 6, 7, (p-1)/2, (p-3)/2, (p-5)/2, (p \pm 1)/3, (p \pm 2)/3, (p \pm 4)/3, (p \pm 5)/3, (p \pm 1)/4, (p \pm 1)/5, (p \pm 2)/5, (p \pm 3)/5, (2p \pm 1)/5, 2(p \pm 1)/5, (2p \pm 3)/5, (p \pm 1)/6, (p \pm 1)/7, (2p \pm 1)/7, (3p \pm 1)/7.$

Table A.4: *Type (iv) examples $Ax^{(p+1)/2}$ mod p from Example 1.5.3*

n	A
3	$1, 2, (p-1)/2$
4	1
5	$1, 2, 3, 4, (p-1)/2, (p-3)/2, (p \pm 1)/3, (p \pm 2)/3, (p \pm 1)/4$
6	$1, 2, 4, (p-1)/2$
7	$1, 2, 3, 4, 5, 6, (p-1)/2, (p-3)/2, (p-5)/2, (p \pm 1)/3, (p \pm 2)/3, (p \pm 4)/3, (p \pm 1)/4, (p \pm 3)/4, (p \pm 1)/5, (p \pm 2)/5, (2p \pm 1)/5, 2(p \pm 1)/5, (p \pm 1)/6$
8	$1, 2, 3, 5, (p-1)/2, (p-3)/2, (p \pm 1)/3, (p \pm 2)/3, (p \pm 1)/5, (2p \pm 1)/5$

Table A.5: *Additional type (iv) examples Ax^k mod p.*

	$k = 1$	$k = (p+1)/2$
$n = 6$	$A = (p+2)/3$	$A = (p-1)/4$

Table A.6: *Largest $p < 10000$ having an $f(x) = Ax$ mod p with $f(I_i) \cap I_j = \phi$ for some (i, j) and A not in Tables A.3 or A.5. (With extra examples for $n = 5$*

	p	A	k	(i, j)
$n = 3$	13	5	1	(2,2)
$n = 4$	19	7	1	(3,4),(4,3))
	19	8	1	(3,3),(4,4)
	29	11	1	(1,4),(3,5)
	29	12	1	(2,2)
	31	7,9	1	(3,3)
$n = 5$	31	12	1	(3,2),(3,4)
	31	13	1	(2,3),(4,3)
	41	9	1	(3,3)
	43	9,19	1	(4,4)
	53	14,19	1	(4,4)
	61	16,22	1	(2,4),(5,3)
$n = 6$	61	19	1	(3,2),(4,5)
	61	25	1	(3,5),(4,2))
$n = 7$	131	27,34	1	(6,6)
$n = 8$	151	31,39	1	(7,8),(8,7)

Table A.7: *Largest* $p < 10000$ *having an* $f(x) = Ax^{(p+1)/2}$ *mod* p *with* $f(I_i) \cap I_j = \phi$ *for some* (i, j) *and* A *not in Tables A.4 or A.5.*

	p	A	k	(i, j)
$n = 3$	17	5	9	(2,2),(3,3)
	17	7	9	(2,3),(3,2)
$n = 4$	61	6	31	(1,3),(4,2)
	61	10	31	(2,4),(3,1)
$n = 5$	137	7	69	(3,2),(4,5)
	137	39	69	(2,4),(5,3)
$n = 6$	197	16	99	(1,3),(4,2)
	197	37	99	(2,4),(3,1)
	277	9,56	139	(5,4),(6,7)
$n = 7$	277	62	139	(4,5),(7,6)
	277	67	139	(5,7),(6,4)
	277	94,123	139	(4,6),(7,5)
$n = 8$	937	188	469	(2,7),(7,2)
	937	314	469	(2,7),(7,7)