Consecutive Elements of Order $n$ in $\mathbb{Z}/q\mathbb{Z}$

Thomas Brazelton\textsuperscript{1}, Joshua Harrington\textsuperscript{2}, Siddarth Kannan\textsuperscript{3}, and Matthew Litman\textsuperscript{4}

\textsuperscript{1}The Johns Hopkins University, \textsuperscript{2}Cedar Crest College, \textsuperscript{3}Pomona College, \textsuperscript{4}Penn State University

Introduction

- The subgroup structure of $\mathbb{F}_q^\times$, the cyclic group of units of $\mathbb{F}_q$, has been well-studied.
- Little is known about the additive gaps between elements of the same multiplicative order.

Research Question

Given $n$, can we guarantee that modulo some prime $q$ we can find adjacent elements of order $n$?

- For prime $q > n$, an element $\alpha \in \mathbb{Z}/q\mathbb{Z}$ has order $n$ if and only if $\alpha$ is a root of $\Phi_n(x)$ in $\mathbb{Z}/q\mathbb{Z}$.
- $\alpha$ and $\alpha + 1$ are both of order $n$ if and only if $\alpha$ is simultaneously a root of $\Phi_n(x)$ and $\Phi_n(x + 1)$.

Example: $\mathbb{Z}/11\mathbb{Z}$

Consider the group of units, $(\mathbb{Z}/11\mathbb{Z})^\times$,

<table>
<thead>
<tr>
<th>$x$</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
</tr>
</thead>
<tbody>
<tr>
<td>ord($x$)</td>
<td>1</td>
<td>10</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>10</td>
<td>10</td>
<td>10</td>
<td>5</td>
<td>2</td>
</tr>
</tbody>
</table>

where the order of $x$, ord($x$), is the smallest positive integer $k$ such that $x^k \equiv 1 \pmod q$.

Here, 3 and 4 are consecutive primitive 5th roots of unity, and 6 and 7 are consecutive primitive 10th roots of unity.

Main Theorem

There exists a prime $q$ such that $\mathbb{Z}/q\mathbb{Z}$ contains consecutive primitive $n$th roots of unity if and only if $n \neq 1, 2, 3, 6$.

- This is equivalent to showing that there exists a prime $q \equiv 1 \pmod n$ dividing the resultant of the cyclotomic polynomials.
- One shows the existence of these primes by factoring the resultant into norms of algebraic integers, and then analyzing the Lucas and Mersenne divisors which arise.

Interesting Corollaries & Propositions

- For $q$ prime, $\mathbb{Z}/q\mathbb{Z}$ has adjacent elements of odd order $n$ if and only if $\mathbb{Z}/q\mathbb{Z}$ contains adjacent elements of order $2n$.
- There does not exist a finite field $\mathbb{Z}/q\mathbb{Z}$ with two adjacent primitive 6th roots of unity.
- The number of fields for which two consecutive elements of order $n$ can exist is less than or equal to $\varphi(n)^2 \frac{\log(3)}{\log(n+1)}$.

Conclusion

We have succeeded in showing that for any $n \neq 1, 2, 3, 6$, we can produce a prime $q > n$ so that there is an element $\alpha \in \mathbb{F}_q$ where both $\alpha$ and $\alpha + 1$ are primitive $n$th roots of unity. Additionally, we have bounded the number of such $q$.

Conjectures

- For $n \neq 1, 2, 3, 6$, all primes $q > n$ dividing $\Gamma_n$ satisfy $q \equiv 1 \pmod n$.
- Let $n \neq 1, 2, 3, 6$, and let $q$ be a prime. Whenever $\alpha$ and $\alpha + 1$ are primitive $n$th roots of unity in a finite field $\mathbb{F}_q$ where $q > n$, we have $\alpha \in \mathbb{F}_q$.

Acknowledgments

- National Science Foundation (grant DMS-1560019)
- Muhlenberg College

Tools

Our work came from the study of the following concepts:

- Cyclotomic Polynomials
- Resultant of Polynomials
- Algebraic Integers and Norms
- Lucas & Mersenne Numbers