Generalized Symmetric Spaces of Dihedral Groups

Tom Edgar

Department of Mathematics
Pacific Lutheran University
Tacoma, WA

Pacific Northwest Meeting of the MAA
University of Portland
April 21, 2012

Introduction, Setup and Notation

Automorphisms and Involutions of D_n

Equivalence classes of Automorphisms of D_n

An Interesting Sequence

Description of Symmetric Spaces of D_n

The work here originated The American Institute of Mathematics.

Began as joint work with Katrina Cunningham (Southern University), Loek Helminck (North Carolina State U.), Benjamin Jones (University of Wisconsin-Stout), Hyunju Oh (Bennet College), and Rachel Schwell (Central Connecticut State), and Jennifer Vasquez (University of Scranton).

Finished with Benjamin Jones and Rachel Schwell.

Basic Setup

Let G be a group.

Let $\theta \in \mathrm{Aut}(G)$ (θ is an automorphism of G)

Important case: $\theta^2 = \mathrm{id}$ (θ is called an involution)

$H = G^\theta = \{g \in G \mid \theta(g) = g\}$ (H is called the fixed point set)

$Q = \left\{g\theta(g)^{-1} \mid g \in G\right\}$

$Q \simeq G/H$ (Q is called the symmetric space)

Classical Example: $G = \mathrm{SL}(n, \mathbb{C})$

Suppose $G = \mathrm{SL}(n, \mathbb{C}) = \{y \in M_n(\mathbb{C}) \mid \det y = 1\}$

Here's an involution of G: $\theta(A) = (A^t)^{-1}$ *"transpose inverse"*

$H = G^\theta = \{g \in G \mid \theta(g) = g\} = \mathrm{SO}(n, \mathbb{C})$ "orthogonal group"

$Q = \left\{y \in M_n(\mathbb{C}) \mid y = y^t,\ \det y = 1\right\}$ *"symmetric matrices"*

Symmetric Spaces for Dihedral Groups

All the definitions make sense for any group.

General Goals:

1. Describe the automorphisms of G up to equivalence.
2. Classify the involutions of G up to equivalence.
3. Given an automorphism (or involution), describe the symmetric space Q and the fixed point set H.
4. Determine the H-orbit structure on Q.
5. Determine the G-orbits on Q and how they split up into H-orbits.

Notation and Terminology

$\mathbb{Z}_n$ - Ring of integers mod n

$U_n = \{a \in \mathbb{Z}_n \mid ay \equiv_n 1 \text{ for some } y \in \mathbb{Z}_n\}$ - units in $\mathbb{Z}_n$

$D_n = \langle r, s \mid s^2 = 1, r^n = 1, sr = r^{n-1}s = r^{-1}s \rangle$

Each element of D_n has a "normal form"

$$D_n = \{1, r, r^2, \ldots, r^{n-1}, s, rs, r^2s, \ldots, r^{n-1}s\}$$

Note: $D_n \cong \mathbb{Z}_n \rtimes \mathbb{Z}_2$ as groups

Note: $\text{Aut}(\mathbb{Z}_n) = U_n$

Notation and Terminology

$\mathbb{Z}_n$ - Ring of integers mod n

$U_n = \{a \in \mathbb{Z}_n \mid ay \equiv_n 1 \text{ for some } y \in \mathbb{Z}_n\}$ - units in $\mathbb{Z}_n$

$D_n = \langle r, s \mid s^2 = 1, r^n = 1, sr = r^{n-1}s = r^{-1}s \rangle$

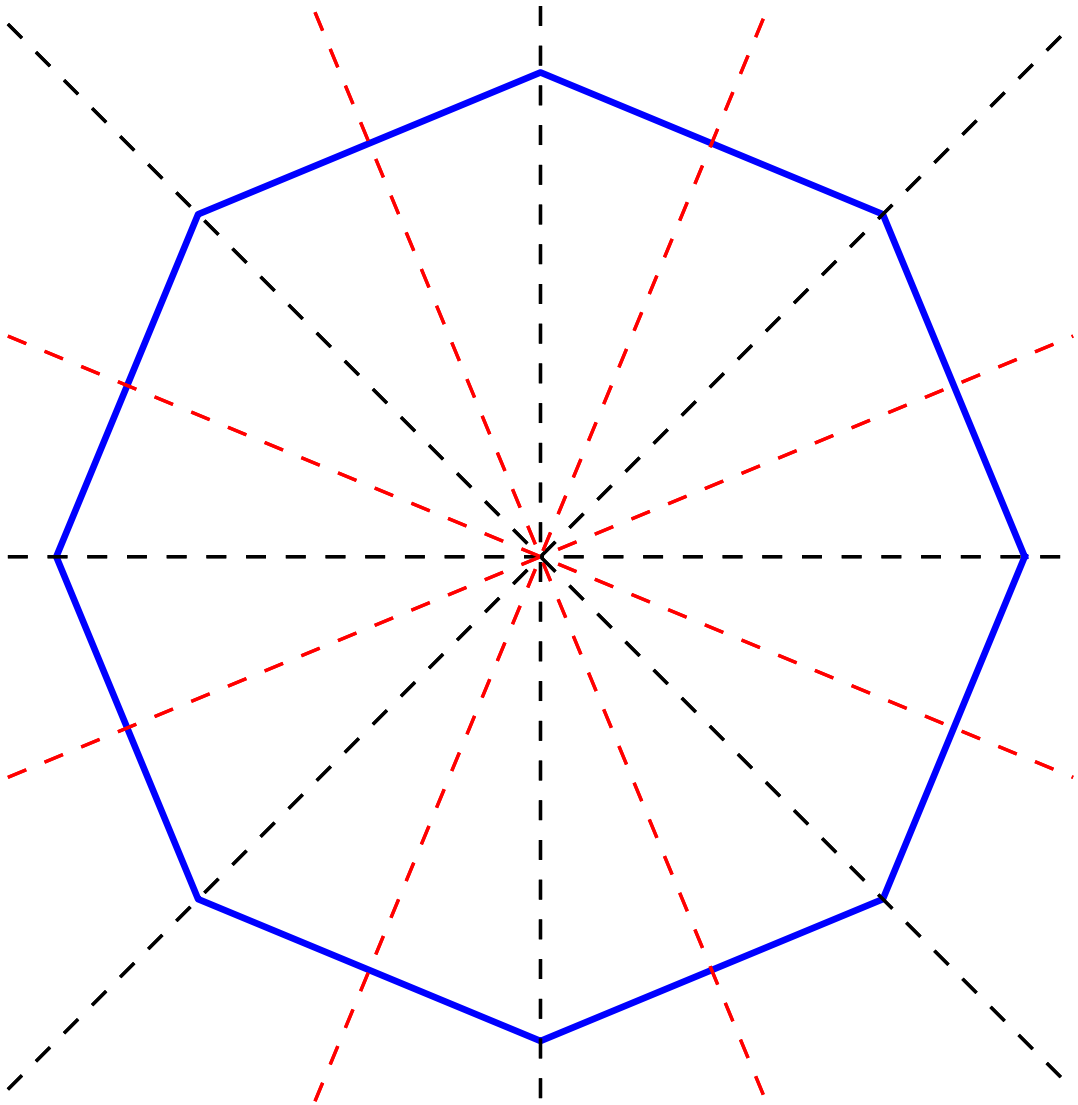
Each element of D_n has a "normal form"

$$D_n = \{1, r, r^2, \ldots, r^{n-1}, s, rs, r^2s, \ldots, r^{n-1}s\}$$

Note: $D_n \cong \mathbb{Z}_n \rtimes \mathbb{Z}_2$ as groups

Note: $\text{Aut}(\mathbb{Z}_n) = U_n$

Symmetry diagram of D_8



Automorphisms and Involutions of D_n

We discovered that the hard work involved in describing symmetric spaces for D_n lies in deeply understanding the structure of the automorphism group of D_n.

We used group theory, elementary number theory, and computer experimentation using Sage[1].

[1] http://www.sagemath.org

Automorphisms and Involutions of D_n

We discovered that the hard work involved in describing symmetric spaces for D_n lies in deeply understanding the structure of the automorphism group of D_n.

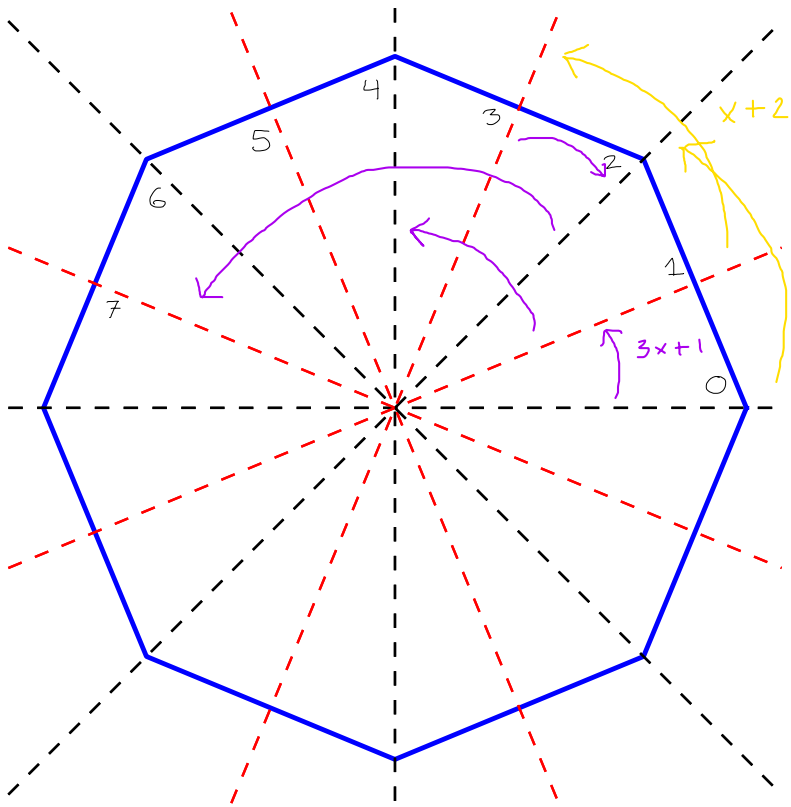
We used group theory, elementary number theory, and computer experimentation using Sage[1].

[1] http://www.sagemath.org

Automorphisms of D_n

$$\mathrm{Aut}(D_n) \cong \{ax + b \mid a \in U_n, b \in \mathbb{Z}_n\}$$

We view the automorphisms as acting on the reflecting planes.



Some Examples

General form: $(ax + b)(r^k s^m) = r^{ak+bm} s^m$

In particular:

conj(s)	$-x$
conj(r)	$x + 2$
Diagram automorphism	$(n-1)x + (n-1)$

Remark: If $ax + b$ is an inner automorphism then $a = \pm 1$

We say θ is *equivalent* to σ if

$$\eta\theta\eta^{-1} = \sigma \text{ for some } \eta \in \mathrm{Aut}(D_n).$$

Check: a is invariant under equivalence.

Some Examples

General form: $(ax + b)(r^k s^m) = r^{ak+bm} s^m$

In particular:

conj(s)	$-x$
conj(r)	$x + 2$
Diagram automorphism	$(n-1)x + (n-1)$

Remark: If $ax + b$ is an inner automorphism then $a = \pm 1$

We say θ is *equivalent* to σ if

$$\eta\theta\eta^{-1} = \sigma \text{ for some } \eta \in \mathrm{Aut}(D_n).$$

Check: a is invariant under equivalence.

Characterizing Automorphisms

If $\theta = ax + b$, then $\theta^k = \mathrm{id}$ if and only if

$$\begin{cases} a^k \equiv 1 & \pmod{n} \\ (a^{k-1} + a^{k-2} + \cdots + 1)b \equiv 0 & \pmod{n} \end{cases}$$

in particular: if $\theta = ax + b$ is an involution then

$$\begin{cases} a^2 \equiv 1 & \pmod{n} \\ (a+1)b \equiv 0 & \pmod{n} \end{cases}$$

Characterizing Automorphisms

If $\theta = ax + b$, then $\theta^k = \mathrm{id}$ if and only if

$$\begin{cases} a^k \equiv 1 & \pmod{n} \\ (a^{k-1} + a^{k-2} + \cdots + 1)b \equiv 0 & \pmod{n} \end{cases}$$

in particular: if $\theta = ax + b$ is an involution then

$$\begin{cases} a^2 \equiv 1 & \pmod{n} \\ (a+1)b \equiv 0 & \pmod{n} \end{cases}$$

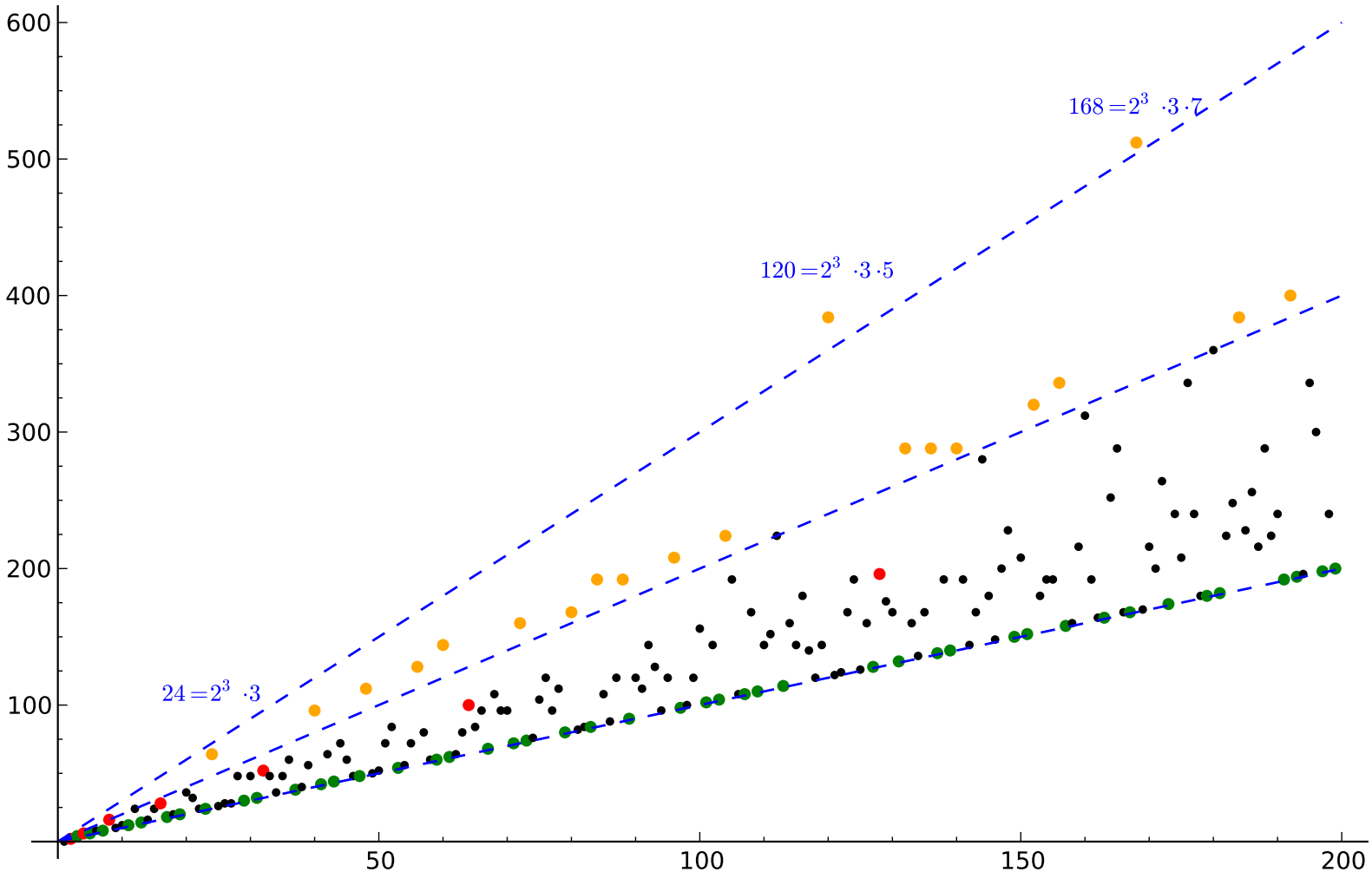
Involutions

To determine the involutions from among all automorphisms,

Solutions to $a^2 \equiv 1 \pmod{n}$ are square roots of unity mod n. Classical number theory tells us the number of these and how to construct them.

Solutions to $(a+1)b \equiv 0 \pmod{n}$ are the zero divisors of $a+1 \in \mathbb{Z}_n$; call this group $\mathrm{ZDiv}(a+1) = \left\langle \frac{n}{\gcd(a+1,n)} \right\rangle \leq \mathbb{Z}_n$.

Number of involutions of D_n vs. n



Equivalence classes of Automorphisms

Let $\mathrm{Aut}_k(D_n) = \{\theta \in \mathrm{Aut}(D_n) \mid \theta^k = \mathrm{id}\}$

Let $\mathrm{ZDiv}(c)$ be the solutions to $cx \equiv 0 \pmod{n}$.

Proposition

The set $Aut_k(D_n)$ is partitioned into equivalence classes indexed by pairs (a, B) where $a^k \equiv 1 \pmod{n}$ and B is an orbit of U_n on $\mathrm{ZDiv}(a^{k-1} + a^{k-2} + \cdots + a + 1)/\langle a - 1\rangle$.

Theorem

Let n be fixed and let $a^k \equiv 1 \pmod{n}$. Then, the number of orbits of U_n on $\mathrm{ZDiv}(a^{k-1} + a^{k-2} + \cdots + a + 1)/\langle a - 1\rangle$ is equal to the number of divisors of

$$\frac{\gcd(a-1, n)\gcd(a^{k-1} + a^{k-2} + \cdots + a + 1, n)}{n}.$$

Equivalence classes of Automorphisms

Let $\mathrm{Aut}_k(D_n) = \{\theta \in \mathrm{Aut}(D_n) \mid \theta^k = \mathrm{id}\}$

Let $\mathrm{ZDiv}(c)$ be the solutions to $cx \equiv 0 \pmod{n}$.

Proposition

The set $Aut_k(D_n)$ is partitioned into equivalence classes indexed by pairs (a, B) where $a^k \equiv 1 \pmod{n}$ and B is an orbit of U_n on $\mathrm{ZDiv}(a^{k-1} + a^{k-2} + \cdots + a + 1)/\langle a - 1\rangle$.

Theorem

Let n be fixed and let $a^k \equiv 1 \pmod{n}$. Then, the number of orbits of U_n on $\mathrm{ZDiv}(a^{k-1} + a^{k-2} + \cdots + a + 1)/\langle a - 1\rangle$ is equal to the number of divisors of

$$\frac{\gcd(a-1, n)\gcd(a^{k-1} + a^{k-2} + \cdots + a + 1, n)}{n}.$$

Equivalence classes of involutions

Theorem

If $\theta = ax + b$ is an involution, then

1. $|\mathrm{ZDiv}(a+1)/\langle a-1\rangle| = \frac{\gcd(a+1,n)\gcd(a-1,n)}{n} \leq 2$
2. *We know when equality holds; equality depends only on the factorization of n and the "type" of a.*

Involutions $ax + b$ and $ax + b'$ are equivalent if $b - b' \in \langle a - 1\rangle$. and they are non-equivalent when b, b' are in different cosets of $\langle a - 1\rangle$ in $\mathrm{ZDiv}(a + 1)$.

Equivalence classes of involutions

Theorem

If $\theta = ax + b$ is an involution, then

1. $|\mathrm{ZDiv}(a+1)/\langle a-1\rangle| = \frac{\gcd(a+1,n)\gcd(a-1,n)}{n} \leq 2$
2. *We know when equality holds; equality depends only on the factorization of n and the "type" of a.*

Involutions $ax + b$ and $ax + b'$ are equivalent if $b - b' \in \langle a - 1\rangle$. and they are non-equivalent when b, b' are in different cosets of $\langle a - 1\rangle$ in $\mathrm{ZDiv}(a + 1)$.

Equivalence classes of involutions

Theorem

If $\theta = ax + b$ is an involution, then

1. $|\mathrm{ZDiv}(a+1)/\langle a-1\rangle| = \frac{\gcd(a+1,n)\gcd(a-1,n)}{n} \leq 2$
2. *We know when equality holds; equality depends only on the factorization of n and the "type" of a.*

Involutions $ax + b$ and $ax + b'$ are equivalent if $b - b' \in \langle a - 1\rangle$. and they are non-equivalent when b, b' are in different cosets of $\langle a - 1\rangle$ in $\mathrm{ZDiv}(a + 1)$.

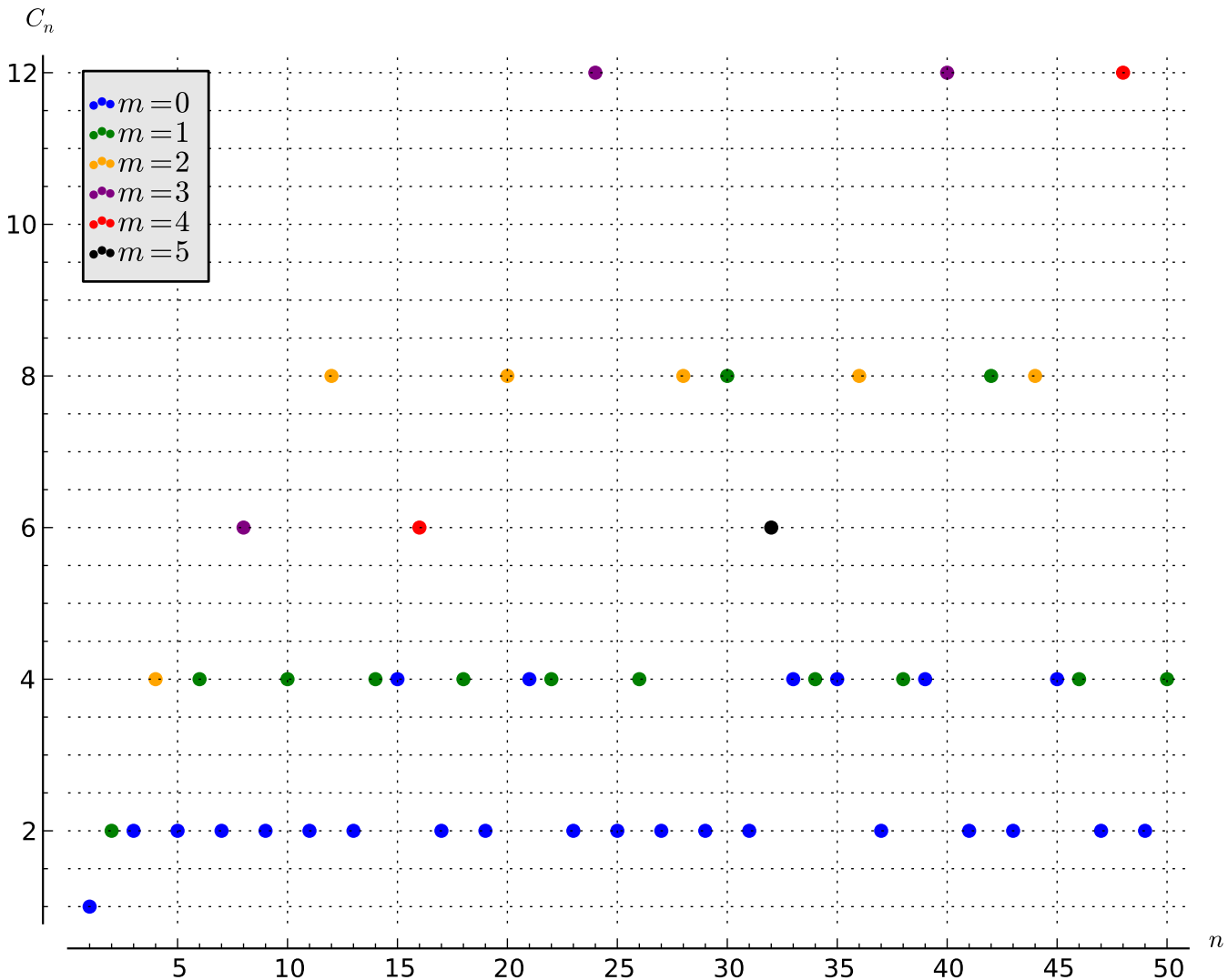
Equivalence classes of involutions

Theorem

Suppose that $n \geq 1$ *and* $n = 2^m p_1^{r_1} \cdots p_k^{r_k}$ *where the* p_i *are distinct odd primes. Then, the number of equivalence classes,* C_n*, of* $\mathrm{Invol}(D_n)$ *is given by*

$$C_n = \begin{cases} 2^{k+m} & \text{if } m < 3 \\ 2^{k+3} - 2^{k+1} & \text{if } m \geq 3. \end{cases}$$

Number of *equivalence classes* of involutions of D_n vs. n



What do you do with a sequence?

The sequence of numbers you get by counting the number of equivalence classes of involutions in D_n versus n is interesting:

1, 2, 2, 4, 2, 4, 2, 6, 2, 4, 2, 8, 2, 4, 4, 6, 2, 4, 2, 8, 4, 4, 2, 12, 2, 4, 2, 8, 2, 8, 2, 6, 4, 4, 4, 8, 2, 4, 4, 12, 2, 8, 2, 8, 4, 4, 2, 12, 2, 4, 4, 8, 2, 4, 4, 12, 4, 4, 2, ...

Check OEIS!

Sequence also counts the number (up to isomorphism) of groups of order $2n$ that have a subgroup isomorphic to $\mathbb{Z}_n$

What do you do with a sequence?

The sequence of numbers you get by counting the number of equivalence classes of involutions in D_n versus n is interesting:

1, 2, 2, 4, 2, 4, 2, 6, 2, 4, 2, 8, 2, 4, 4, 6, 2, 4, 2, 8, 4, 4, 2, 12, 2, 4, 2, 8, 2, 8, 2, 6, 4, 4, 4, 8, 2, 4, 4, 12, 2, 8, 2, 8, 4, 4, 2, 12, 2, 4, 4, 8, 2, 4, 4, 12, 4, 4, 2, ...

Check OEIS!

Sequence also counts the number (up to isomorphism) of groups of order $2n$ that have a subgroup isomorphic to $\mathbb{Z}_n$

With equivalence of automorphisms understood, describing the symmetric space is relatively easy:

Theorem

Let $G = D_n$ and $\theta = ax + b \in Aut(D_n)$ be of finite order. Then

$$H = \{r^k \mid k(a-1) \equiv 0 \ (mod\ n)\} \cup \{r^k s \mid k(a-1) \equiv -b \ (mod\ n)\}$$
$$Q = \{r^k \mid k \in \langle a-1 \rangle \cup (-b + \langle a-1 \rangle)\}.$$

Corollary

Let $\theta = ax + b$.

1. *H is either $\mathrm{ZDiv}(a-1)$ or $\mathrm{ZDiv}(a-1) \rtimes \mathbb{Z}_2$.*
2. *Q is a subgroup if $b \in \langle a-1 \rangle$ and in this case $Q \cong \langle a-1 \rangle$.*
3. *If θ is an involution Q is always a subgroup.*

With equivalence of automorphisms understood, describing the symmetric space is relatively easy:

Theorem

Let $G = D_n$ and $\theta = ax + b \in Aut(D_n)$ be of finite order. Then

$$H = \{r^k \mid k(a-1) \equiv 0 \ (mod\ n)\} \cup \{r^k s \mid k(a-1) \equiv -b \ (mod\ n)\}$$
$$Q = \{r^k \mid k \in \langle a-1 \rangle \cup (-b + \langle a-1 \rangle)\}.$$

Corollary

Let $\theta = ax + b$.

1. *H is either $\mathrm{ZDiv}(a-1)$ or $\mathrm{ZDiv}(a-1) \rtimes \mathbb{Z}_2$.*
2. *Q is a subgroup if $b \in \langle a-1 \rangle$ and in this case $Q \cong \langle a-1 \rangle$.*
3. *If θ is an involution Q is always a subgroup.*

THANKS!

Any Questions?

References

On the Structure of Involutions and Symmetric Spaces of Dihedral Groups.