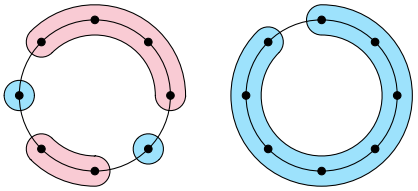
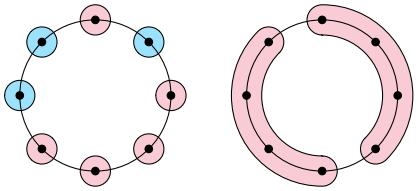
Rotational symmetries and Gauss congruence



Fern Gossow

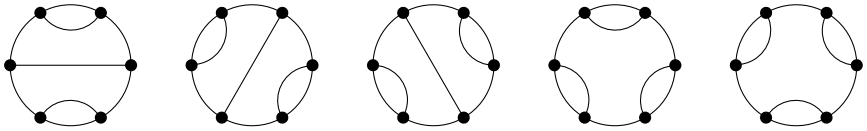
QTMC 2025



Introduction. This is an overview of my research on rotational symmetries and Gauss congruence which I am presenting at QTMC 2025. You can find the full work on the arXiv. There are lots of directions that this work could still go, so please reach out if you would like to collaborate!

Background

As a combinatorist, you probably have a favourite integer sequence, and a sequence of sets it enumerates. For example, if your favourite numbers are the Catalan numbers you might know about non-crossing matchings.



If X_n is the set of non-crossing matchings on n vertices, then we have

$$a_n := \#X_n = \begin{cases} \mathrm{Cat}_{n/2} & \text{if } n \text{ even,} \\ 0 & \text{otherwise.} \end{cases}$$

Many integer sequences also have polynomial analogues, usually called q-analogues. For the Catalan numbers, we set $[n]_q := 1 + q + \cdots + q^{n-1}$ for every $n \geq 1$ and

$$[\mathrm{Cat}_n]_q = \frac{1}{[n+1]_q} \begin{bmatrix} 2n \\ n \end{bmatrix}_q = \frac{1}{[n+1]_q} \frac{[2n]_q \cdots [2]_q [1]_q}{[n]_q \cdots [1]_q [n]_q \cdots [1]_q}.$$

It turns out that the denominator always cancels, so these are integer polynomials. We define a polynomial analogue of a_n by $f_n(q) := [\mathrm{Cat}_{n/2}]_q$ when n is even and $f_n(q) := 0$ otherwise.

A natural question is whether there is a relation between the set analogue X_n and the polynomial analogue $f_n(q)$. The answer is a resounding yes!

Theorem. Let $X_{n;d}$ be the set of non-crossing matchings on n vertices with d-fold rotational symmetry. The number of such elements is given by the polynomial evaluation

$$\#X_{n;d} = f_n(\zeta_d)$$

for every $d \mid n$, where ζ_d is the primitive d^{th} root of unity $e^{2\pi i/d}$.

For example, $f_6(q) = 1+q^2+q^3+q^4+q^6$ and $f_6(\zeta_2) = f_6(-1) = 3$ counts the number of non-crossing matchings on six vertices with 2-fold rotational symmetry.

(Personal) motivation

The relation between X_n and $f_n(q)$ above is an example of the cyclic sieving phenomenon, which has become a popular theme in enumerative combinatorics since it was first described in the 2000s. I learnt about it during my first meeting with my Honours supervisor, where I was shown the following theorem of Rhoades (2010).

Theorem. Let $\lambda \vdash n$ be a rectangular partition and X_λ the set of standard Young tableaux with shape λ. Suppose the cyclic group C_n acts on X_λ by the jeu de taquin promotion map, and let $f_\lambda(q)$ be the following q-analogue to the classical hook length formula:

$$f_\lambda(q) = \frac{[n]_q \cdots [1]_q}{\prod_{x\in\lambda}[h(x)]_q}.$$

Then the number of tableaux with d-fold rotational symmetry under this action is $f_\lambda(\zeta_d)$.

What a miracle! When λ is a rectangle of size $2 \times n$, there is a natural bijection beween standard Young tableaux and non-crossing matchings, and we recover our first example as a corollary.

Since seeing this theorem, it became a dream of mine to prove a cyclic sieving result of my own. I also wanted to build understanding of *why* cyclic sieving results happen, because many proofs in the literature are calculation-heavy and lack conceptual motivation.

Key idea

To summarise, we want to find a sequence of sets (X_n) and a sequence of polynomials $(f_n(q))$, such that the subset $X_{n;d} \subseteq X_n$ of elements having d-fold rotational symmetry under some natural rotation action is counted by $f_n(\zeta_d)$ for every $d \mid n$.

When solving a hard *existence* problem, a common trick is to add constraints which provide additional structure. This was the key idea which sparked this project.

Assumption. For every $d \mid n$, we have $\#X_{n;d} = \#X_{n/d}$.

Known results

Examples of cyclic sieving phenomena satisfying this assumption were termed *Lyndon-like sieving* in work by Alexandersson, Linusson and Potka (2019), due to an initial example involving Lyndon words. By classical theory of rotational symmetries, under the assumption, the enumerating sequence (a_n) given by $a_n := \#X_n$ satisfies the condition of Gauss congruence, meaning

$$\frac{1}{n}\sum_{d|n} \mu(d) a_{n/d} \in \mathbb{Z}$$

for every $n \geq 1$, where μ is the number-theoretic Möbius function. Intriguingly, a sequence (a_n) satisfies Gauss congruence if and only if there is an integer sequence (c_n), which we call the *colour sequence* (more on this later!), such for every $n \geq 1$:

$$a_n = c_1 a_{n-1} + c_2 a_{n-2} + \cdots + c_{n-1} a_1 + n c_n. \qquad (\heartsuit)$$

This fact often goes unmentioned in papers about Gauss congruence[1], but will be very important for the construction of our sets X_n.

On the polynomial side, the assumption that $\#X_{n;d} = \#X_{n/d}$ for every $d \mid n$ translates to the arithmetic identity $f_n(\zeta_d) = f_{n/d}(1)$. Gorodetsky (2019) proved that this condition is equivalent to requiring that

$$\frac{1}{[n]_q} \sum_{d|n} \mu(d) f_{n/d}(q) \in \mathbb{Z}[q]$$

for every $n \geq 1$. Observe that this is simply a q-analogue of Gauss congruence.

In fact, if (X_n) is *any* sequence of sets satisfying the assumption, and $(f_n(q))$ is *any* sequence of integer polynomials satisfying q-Gauss congruence such that $f_n(1) = \#X_n$ for every $n \geq 1$, then we obtain an example of the cyclic sieving phenomenon.

Main result

The main result of my paper is a general method for obtaining examples of the above. Finding sequences satisfying Gauss congruence is easy: just scrape the OEIS. I give multiple methods for finding a q-Gauss congruence $(f_n(q))$ which specialises to a given Gauss congruence (a_n) under $q = 1$, all of which are new, but too tedious to cover here.

Instead, we will focus on constructing the sets (X_n) using a novel combinatorial object called a *festoon*. Fixing a nonnegative integer sequence (c_i), a festoon of size n is a circular arrangement of beads with total length n, where beads of length i are coloured in one of c_i ways. If $c_n = 2$ for every $n \geq 1$, then the title image gives examples of festoons of size 8. The main theorem exemplifies the cyclic sieving phenomenon for an arbtirary colour sequence, and we give specific examples of this in the next section.

Theorem. Let (a_n) be a Gauss congruence whose colour sequence (c_n) from (♡) is nonnegative, and $(f_n(q))$ an associated q-Gauss congruence. Let X_n be the set of festoons of size n. Then the number of such festoons with d-fold rotational symmetry for every $d \mid n$ is

$$\#X_{n;d} = \#X_{n/d} = a_{n/d} = f_{n/d}(1) = f_n(\zeta_d)$$

so we obtain an example of the cyclic sieving phenomenon.

Examples

Necklaces

If $(c_n) = (\gamma, 0, 0, \dots)$, then (♡) gives $a_1 = \gamma$ and $a_n = \gamma a_{n-1}$ for $n > 1$, so $a_n = \gamma^n$. The set X_n is the set of necklaces with n beads, with each coloured in one of γ ways.

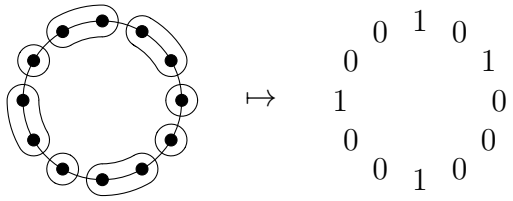
[1] Literature is hard to track down because there are many competing names for sequences satisfying Gauss congruence, such as Gauss sequences, Newton sequences, Fermat sequences, double Fermat sequences and Dold sequences. We have of course solved the issue.

Lucas numbers

If $(c_n) = (1, 1, 0, 0, \dots)$, then (♡) gives $a_1 = 1$, $a_2 = 3$ and $a_n = a_{n-1} + a_{n-2}$ for $n > 2$, so a_n are the Lucas numbers. If we colour the two beads as

$$\textcircled{0} \qquad \text{and} \qquad \textcircled{0\ 1}$$

then X_n becomes cyclic binary words of length n where the 1s are never adjacent.

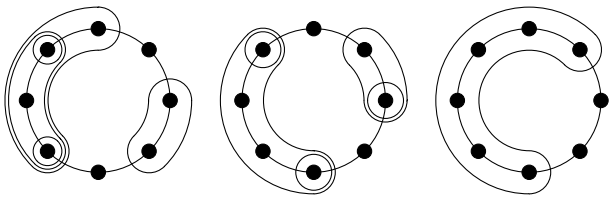


In this case the q-Gauss congruence we obtain with our methods is

$$f_n(q) = \sum_{k=0}^{\lfloor n/2 \rfloor} \frac{[n]_q}{[n-k]_q} \begin{bmatrix} n-k \\ k \end{bmatrix}_q.$$

Central Delannoy numbers

If $c_n = \mathrm{sch}_{n-1}$ where sch_n are the small Schröder numbers, then (a_n) is the sequence of central Delannoy numbers, which count the number of tubings on the cycle graph with n vertices. We prove this both with a novel bijection, and using the theory of Riordan arrays.



The associated q-Gauss congruence in this case is

$$\sum_{k=0}^{n-1} \begin{bmatrix} n+k-1 \\ k \end{bmatrix}_q \begin{bmatrix} n-1 \\ k \end{bmatrix}_q.$$

Refining counts

The polynomials in the previous two examples involve a sum over k. Both have combinatorial meaning, counting the number of ones in each binary word and the number of tubes in each tubing respectively. Our methods allow us to describe cyclic sieving phenomena indexed by parameters.

For example, if $X_{n,n_1,n_2,\dots}$ is the set of festoons of size $n = n_1 + 2n_2 + 3n_3 + \cdots$ containing n_i monocoloured beads of length i for every $i \geq 1$, we obtain a cyclic phenomenon with

$$f_{n,n_1,n_2,\dots}(q) = \frac{[n]_q}{[n_1 + n_2 + \cdots]_q} \begin{bmatrix} n_1 + n_2 + \cdots \\ n_1, n_2, \dots \end{bmatrix}_q.$$

Further directions

Here is a sketch of other results which appear in the work, and ideas for future research. Please talk to me if you are interested in this kind of thing, I would love to collaborate!

More examples

The OEIS has many more examples of Gauss congruences for which it is not obvious what a combinatorially-natural set X_n should be, other than the brute-force festoon description.

For example, if a_n is the number of solutions to $x^2 + y^2 + z^2 + w^2 = n$, then (a_n) satisfies Gauss congruence. This is the Θ-series for the lattice $\mathbb{Z}^4$, so take X_n to be the set of points in $\mathbb{Z}^4$ with a square-distance from the origin of n. How do we find a natural action of the cyclic group which satisfies our assumption?

Gauss congruences from matrices

If M is an integer matrix, then $a_n = \operatorname{tr}(M^n)$ satisfies Gauss congruence. Gorodetsky observed that we get a q-Gauss congruence for the Lucas numbers by taking

$$f_n(q) = \operatorname{tr}\left(\begin{bmatrix}0 & 1\\ 1 & 1\end{bmatrix}\begin{bmatrix}0 & q\\ 1 & 1\end{bmatrix}\cdots\begin{bmatrix}0 & q^{n-1}\\ 1 & 1\end{bmatrix}\right).$$

Can we do this in general? Is it possible to determine an appropriate q-analogue $M(q)$ with $M(1) = M$ such that $\operatorname{tr}(M(1)M(q)\cdots M(q^{n-1}))$ satisfies q-Gauss congruence?

Negative colour values

There are plenty of important Gauss congruences which have negative c_n values. We don't get the cyclic sieving phenomenon anymore, but by counting *signed festoons* (which are negative when they contain an odd number of 'negative' beads), we can still find a set analogue. Can we develop this theory further?

Semigroups

We extend our notion of Gauss congruence to sequences indexed not just by the positive integers, but by a ranked semigroup with finite decomposition. Using this theory, many well-known examples of cyclic sieving turn out to satisfy our assumption, just under a different semigroup.

Most examples simply involve adding new parameters, as we discussed in the previous section. Can we find less trivial examples of this?

Other congruences

The Catalan-based cyclic sieving described in our first section does not satisfy Gauss congruence. Is there a similar Catalan-type theory that can be developed? What is the appropriate notion of congruence, and how do we find the q-analogue? Which well-known examples of cyclic sieving fit into these different types of congruences?