Alabama Journal of Mathematics

Alabama Journal of Mathematics
Volume 45 (1) (2022), 1 – 9
DOI : 10.10001/ajm

Original Article

The Spider and the Fly

Cornelius Pillen*[1]

[1] *Department of Mathematics and Statistics*
University of South Alabama
Mobile, AL 36688, USA

Abstract

The spider and the fly are sitting in the coordinate plane. The spider's coordinates are $(2018, 6903)$ and the fly sits at $(2561, 2353)$. The spider is no ordinary spider. It discreetly spins its web by moving in four different directions. Starting from a point with integer coordinates (a, b), the spider can jump to $(a + b, b)$, $(a - b, b)$, $(a, b + a)$, or $(a, b - a)$. The fly is terrified and sits perfectly still. Will the spider ever catch the fly?

After we present and represent the spider group we look at the spider's orbit and count the prime locations. Finally, the spider's moves reveal a surprising connection with modular representation theory of algebraic groups.

Mathematics Subject Classification (2020). 11-01, 20-01, 20G05

Keywords. Math Circles, Euclidean Algorithm, Modular Group, Modular Representation Theory

Will you walk into my parlour, said a Spider to a Fly;

- Mary Howett (1799 – 1888)

Then I said my, my, like a spider to a fly
Jump right ahead in my web.

- Mick Jagger, Keith Richards

1. Introduction

This article is based on my Lewis Parker Lecture that was presented on March 2, 2019 at Huntingdon College. I would like to thank the AACTM for inviting me. I greatly enjoyed the meeting. The following write-up starts with one of my favorite problems from the Mobile Mathematics Circle, visits some fundamental ideas in group theory, encounters some recent results and open problems in number theory, and finally weaves its way into my area of research, modular representation theory of finite groups of Lie type and algebraic groups.

*Corresponding Author.
Email addresses: pillen@southalabama.edu
Received: June 3, 2020; Accepted: January 7, 2021

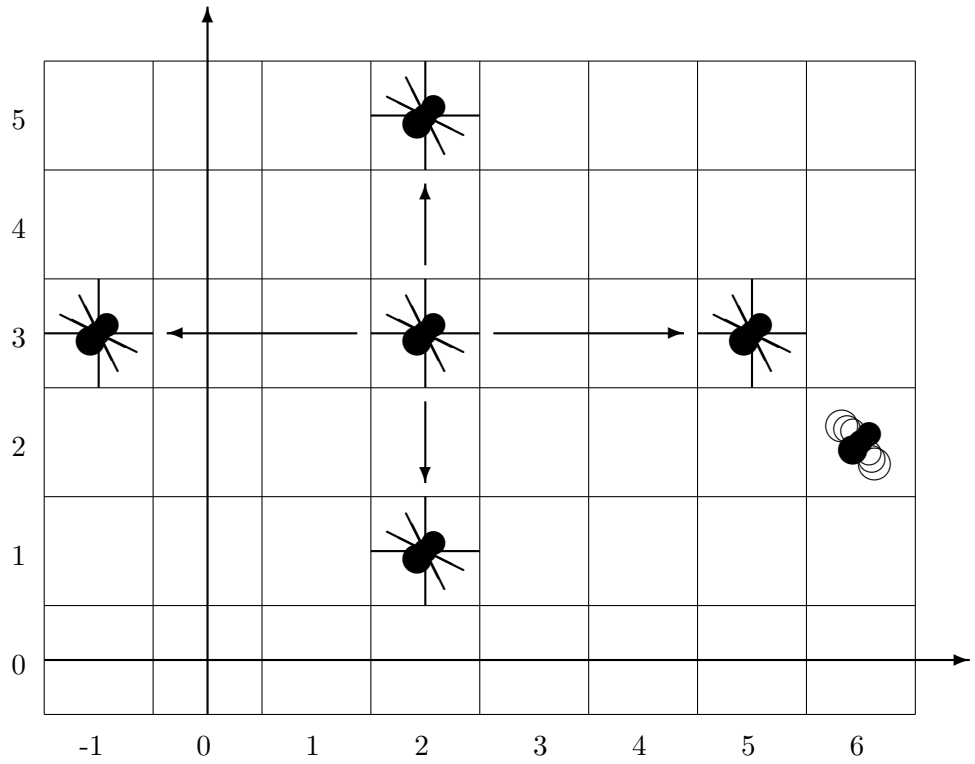
This is an expository article. There are no proofs and no original ideas. I tried not to get lost in technical details (except possibly in Section 3). Hopefully, the reader will be able to get a flavor of the rich mathematics that lies below it all. In the end it is really just about $\mathrm{SL}_2(\mathbb{Z})$.

2. Problems from the Mobile Mathematics Circle

More than 20 years ago my colleagues Vasiliy Prokhorov and Dan Flath started the Mobile Math Circle, a weekly event for local high school and middle school students, who solve math problems under the guidance of professional mathematicians. I have been leading sessions of the Math Circle for many years and one of my favorite problems is the following:

Spider and Fly: *The spider and the fly are sitting in the coordinate plane. The spider's coordinates are* $(2018, 6903)$ *and the fly sits at* $(2561, 2353)$*. The spider is no ordinary spider. It discreetly spins its web by moving in four different directions. Starting from a point with integer coordinates* (a, b)*, the spider can jump to* $(a + b, b)$*,* $(a - b, b)$*,* $(a, b+a)$*, or* $(a, b-a)$*. The fly is terrified and sits perfectly still. Will the spider ever catch the fly?*

The answer of course is either "yes" or "no". We have a 50% chance of getting it right. But we are mainly interested in finding a justification of our answer. To simplify the problem, let us consider some smaller numbers for the starting positions. Let the spider start at $(2, 3)$ and the fly sits at $(6, 2)$. Will the spider ever reach the fly? We don't care how many jumps it might take. The picture below illustrates the situation.



This is a classical **invariant problem**. All the possible points that the spider can reach will have one common value, the invariant. The observant reader probably recognized that the invariant is the greatest common divisor (gcd) of the initial position $(2, 3)$, namely 1. More generally, a spider sitting at (a, b) can only reach points (c, d) with

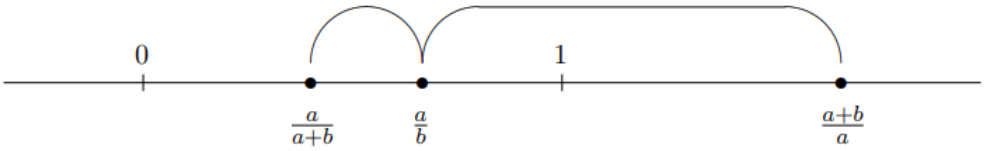
$\gcd(a,b) = \gcd(c,d)$. The reason is a well-known fact from elementary number theory: If not both, a and b, are equal to zero, then $\gcd(a,b) = \gcd(a,a+b)$.
Borrowing a term from group theory one can show that the **orbit** of a spider starting at (a,b), i.e. the set of all points that the spider can reach, is

$\mathcal{O}(a,b) = \{(c,d) \in \mathbb{Z} \times \mathbb{Z} \mid \gcd(a,b) = \gcd(c,d)\}$.

Since the $\gcd(6,2) = 2 \neq 1$, we see that the fly in our example is perfectly safe. I will leave it to the reader to find a solution to the originally stated problem (without using a calculator or computer). Consulting a spider that spent some time in Euclid's house might be helpful here.

There is an interesting variation of the above theme. This time we are dealing with a rational spider.

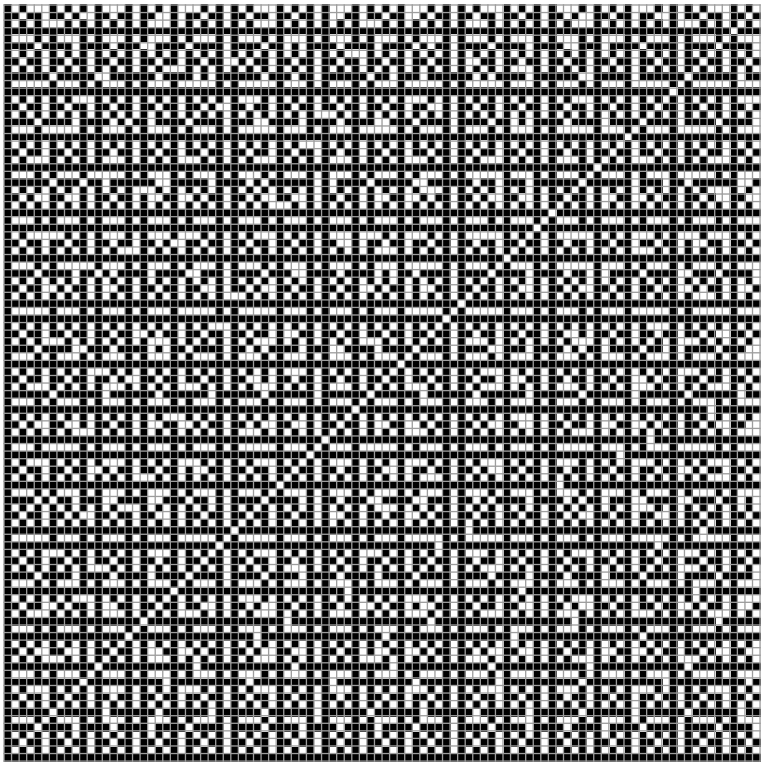
The Rational Spider: *If the rational spider sits at a rational point $\frac{a}{b}$ on the positive part of the number line it can jump either to the point $\frac{a+b}{b}$ or to the point $\frac{a}{a+b}$. Are there any points on the positive part of the number line for a fly to hide, if the rational spider sits at 1?*



Finally, I would like to mention a game that we like to play and explore during our Math Circle sessions. The game was invented by Cole and Davie [3].

Euclid's Game *A pair of positive numbers is written on the board. Two players move alternately, subtracting from the greater entry a positive integer multiple of the smaller one, as long as the result remains positive. The player who is unable to make a move loses. Is there a winning strategy?*

I want to conclude this section with the picture below. It shows the part of the orbit of a spider starting at $(1,1)$ that lies in the first quadrant. Squares that the spider can reach are dark and squares that are safe for a fly are light. Do you recognize any patterns or symmetries?



3. The Free Spider Group, Presentations and Representations

In this section we want to explore the movement of the spider using the language of group theory. Please note that the exposition tries to give a flavor of the underlying mathematics rather than being a rigorous introduction.

3.1. The Free Spider Groups

Recall the "spider moves". The move that adds the second coordinate to the first coordinate is denoted by X :

$$(a,b) \xrightarrow{X} (a+b,b)$$

The move that subtracts the second coordinate to the first coordinate is denoted by X^{-1}.

$$(a,b) \xrightarrow{X^{-1}} (a-b,b)$$

Note that this notation makes sense because X^{-1} undoes X. It is the **inverse**.

$$(a,b) \xrightarrow{X} (a+b,b) \xrightarrow{X^{-1}} (a,b) \text{ and } (a,b) \xrightarrow{X^{-1}} (a-b,b) \xrightarrow{X} (a,b).$$

Similarly, we introduce the moves Y and Y^{-1} such that

$$(a,b) \xrightarrow{Y} (a,a+b) \xrightarrow{Y^{-1}} (a,b) \text{ and } (a,b) \xrightarrow{Y^{-1}} (b,b-a) \xrightarrow{Y} (a,b).$$

A "spider path" is just a sequence of moves that can be described as a **word** made from the letters X, Y and their inverses X^{-1}, Y^{-1}. Whenever a letter is followed by its inverse or follows its inverse we can omit the pair. For example

$$YXY^{-1}XY^{-1}XX^{-1}YX^{-1}Y = YXY^{-1}XY^{-1}\,(XX^{-1})\,YX^{-1}Y$$

can be simplified to

$$YXY^{-1}X\,(Y^{-1}Y)\,X^{-1}Y = YXY^{-1}\,(XX^{-1})\,Y = YX\,(Y^{-1}Y) = YX.$$

We call the last expression a **reduced word** because no further cancellations are possible.

The **Free Spider Group** G is defined to be the set of all reduced words in X, Y and their inverses, X^{-1}, Y^{-1}, together with the binary operation "pasting words together", followed by reductions, if possible. The identity is the empty word.
Here is an example. "Multiplying" the word $XY^{-1}XXY$ by $Y^{-1}X^{-1}YYX^{-1}$ yields:

$$\begin{aligned}(XY^{-1}XXY)\cdot(Y^{-1}X^{-1}YYX^{-1}) &= XY^{-1}X\,(X(YY^{-1})X^{-1})\,YYX^{-1}\\ &= XY^{-1}XYYX^{-1}\end{aligned}$$

3.2. Spider Actions and Presentations

But does the Free Spider Group really capture the spider's movements?
We say the group G **acts** on the set $\{(a,b) \mid a,b \in \mathbb{Z}\}$ as follows.

$$X\cdot(a,b) = (a+b,b) \text{ and } Y\cdot(a,b) = (a,a+b).$$

Note that

$$X^{-1}\cdot(a,b) = (a-b,b),\ Y^{-1}\cdot(a,b) = (a,b-a),\ \text{and } (vw)\cdot(a,b) = v\cdot(w\cdot(a,b)),$$

for all words v and w. We call this a **group action**.

Let us have a look at the action of various words. Where does the word $YX^{-1}Y$ send a spider sitting at (a,b)?

$$\text{The Answer: } (a,b) \xrightarrow{Y} (a,a+b) \xrightarrow{X^{-1}} (-b,a+b) \xrightarrow{Y} (-b,a)$$

The following shows that the path corresponding to the word $(YX^{-1}Y)^4$ sends every spider back to the point at which it started.

$$(a,b) \xrightarrow{YX^{-1}Y} (-b,a) \xrightarrow{YX^{-1}Y} (-a,-b) \xrightarrow{YX^{-1}Y} (b,-a) \xrightarrow{YX^{-1}Y} (a,b).$$

Exercise: Show that the path corresponding to the word $(Y^{-1}X)^3$ leads to the same location as the one corresponding to $(YX^{-1}Y)^2$.

We would like to find a new group where distinct elements result in distinct "spider paths" and every "spider path" corresponds to an element. The above observations tell us that whenever we have a word in the free spider group that contains the sub-word $(YX^{-1}Y)^4$ we can simply delete the sub-word. Similarly, we can always replace the sub-word $(Y^{-1}X)^3$ by $(YX^{-1}Y)^2$ and vice versa. Such rules are called relations. Using our original generators X and Y we describe a new group H as follows:

$$H = \langle \underbrace{X,Y}_{generators} \mid \underbrace{(YX^{-1}Y)^4 = 1, (Y^{-1}X)^3 = (YX^{-1}Y)^2}_{relations} \rangle$$

We call this a **presentation** of H.

If one chooses $S = YX^{-1}Y$ and $U = Y^{-1}X$, one may rewrite the above in a simplified form as

$$H = \langle \underbrace{S,U}_{generators} \mid \underbrace{S^4 = 1, U^3 = S^2}_{relations} \rangle.$$

At this point it could be quite possible that there are more relations that we have not seen. We will have to take a second look at the spider actions.

3.3. Representations

Is there a better way of describing the spider action? We start with some cosmetic changes, switching to column vectors. Recall that

$$X\cdot\begin{bmatrix} a \\ b \end{bmatrix} = \begin{bmatrix} a+b \\ b \end{bmatrix} \text{ and that } Y\cdot\begin{bmatrix} a \\ b \end{bmatrix} = \begin{bmatrix} a \\ a+b \end{bmatrix}.$$

That would suggest that

$$X \cdot \begin{bmatrix} a \\ b \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} a \\ b \end{bmatrix} \text{ and that } Y \cdot \begin{bmatrix} a \\ b \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} a \\ b \end{bmatrix}$$

This observations suggest a map from the Free Spider Group to the set of invertible 2×2 matrices with integer entries. Indeed, we define $\phi : G \to \mathrm{GL}_2(\mathbb{R})$ via

$$\phi(X) = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \text{ and } \phi(Y) = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}.$$

Moreover, we want that $\phi(v \cdot w) = \phi(v)\phi(w)$, for any pair of words $v, w \in G$. The map ϕ is a group homomorphism. We call this a **representation** of G. Jim Humphreys writes in [4] "A representation provides a sort of picture of G: in place of abstract group elements, multiplied abstractly, we get concrete matrices, multiplied in a familiar way".

Exercises: Find $\phi((YX^{-1}Y)^4)$, $\phi((Y^{-1}X)^3)$ and $\phi((YX^{-1}Y)^2)$.

It turns out that $\phi((YX^{-1}Y)^4)$ is simply the identity matrix and that $\phi((Y^{-1}X)^3) = \phi((YX^{-1}Y)^2)$. This implies that one actually obtains a representation not just of of G but also of H.

A natural question to ask is: What is the image or the range of ϕ? Any matrix that is contained in the image of ϕ is a product of the matrices

$$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}, \begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ -1 & 1 \end{bmatrix}.$$

All of these have determinant one and integer entries. The image of ϕ is therefore contained in $\mathrm{SL}_2(\mathbb{Z})$, the set of 2×2 integer matrices with determinant 1.

Do we get all the matrices in $\mathrm{SL}_2(\mathbb{Z})$? Indeed, we do. One can find a simple argument using elementary matrices. Without proof I will list some "spider facts" that show that the group of "spider paths" is indeed the group $\mathrm{SL}_2(\mathbb{Z})$.

- There is a one-to-one correspondence between the "spider paths" and the elements of $\mathrm{SL}_2(\mathbb{Z})$.
- H is isomorphic to $\mathrm{SL}(2, \mathbb{Z})$, or equivalently,

$$\langle\, X, Y \mid (YX^{-1}Y)^4 = 1, (Y^{-1}X)^3 = (YX^{-1}Y)^2 \,\rangle \text{ and } \langle\, S, U \mid S^4 = 1, U^3 = S^2 \,\rangle$$

  are presentation of $\mathrm{SL}_2(\mathbb{Z})$ (For more detail see [5]).

We have now seen that the movements of the spider that we encountered in the Math Circle can be best described via the group $\mathrm{SL}_2(\mathbb{Z})$, a group that features prominently in many areas of mathematics, especially in number theory.

4. Prime Locations

In this section we will recall some well-known facts from number theory and quote a fairly recent theorem. These observations lead to surprising results in modular representation theory of algebraic groups. These will be discussed in the last section of the paper.

Let us consider a spider that is out for an infinite walk.

$$(1,0) \xrightarrow{Y} (1,1) \xrightarrow{X} (2,1) \xrightarrow{Y} (2,3) \xrightarrow{X} (5,3) \xrightarrow{Y} (5,8) \xrightarrow{X} (13,8) \xrightarrow{Y} \ldots.$$

The reader might recognize that the coordinates of the points visited by the spider along this infinite path contain the Fibonacci numbers. A theorem dating back to 1913 by the American mathematician Carmichael says the following:

Theorem 4.1 (R. D. Carmichael)**.** *For n greater than 12, the nth Fibonacci number has at least one prime factor that does not divide any earlier Fibonacci number.*

Carmichael was born in Goodwater, Alabama, and spent most of his academic career at the University of Illinois. Carmichael's Theorem implies that, for n sufficiently large, the first n Fibonacci numbers have at least n distinct prime divisors. For the spider this implies that, for large n, after the first n steps of its stroll every step will let it visit a point whose coordinates produce a new prime factor.

It is still an open question whether infinitely many Fibonacci numbers are prime. So we don't know whether our spider will actually visit infinitely many "prime locations". However, if we allow for "spider paths" that correspond to arbitrary words in X and Y we can do a lot better.

A recent theorem due to Kontorovich, McNamara and Williamson [7, Appendix] shows that for sufficiently large n there exist "spider paths" of length at most n in X and Y (no inverses) that produce not only prime factors but actual primes. Not only do these primes grow exponentially in terms of the path length n but the number of such primes also grows exponentially. Here is a slightly reworded statement of the theorem.

Theorem 4.2 (A. Kontorovich, P. J. McNamara and G. Williamson)**.** *There exist absolute constants $\tau > 0$ and $c > 1$ such that, for all n large, there exists a word w in X and Y of length at most n with $w \cdot (1,0) = (p, *)$, where p is a prime and $p > \tau c^n$. Moreover,*

$$\#\{\text{ primes } p > \tau c^n \mid \exists \text{ a path } w \text{ of length} \leq n \text{ with } w \cdot (1,0) = (p,*)\} \gg \frac{c^n}{n}.$$

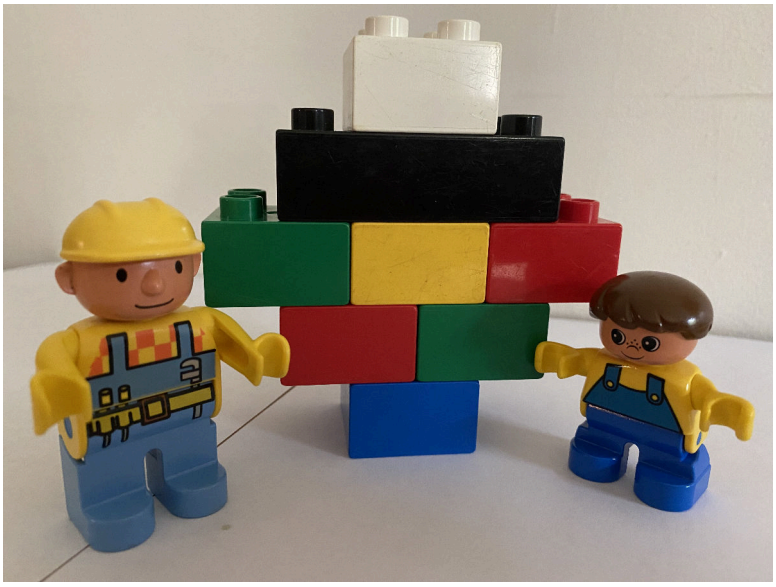
The notation $f(n) \gg g(n)$ means that $|g(n)| \leq M|f(n)|$ for a fixed $0 < M$ and large n.

5. Modular Representation Theory

Fix a prime p. We denote by $\mathbb{F}_p$ the field with p elements and by k an algebraically closed field containing $\mathbb{F}_p$. In this section we want to look at finite-dimensional modular representations of finite groups of Lie type, algebraic groups, and Lie algebras.

We limit the exposition to the following examples: $\mathrm{SL}_n(\mathbb{F}_p)$, the finite group consisting of all $n \times n$ matrices with entries in $\mathbb{F}_p$ and determinant one, $\mathrm{SL}_n(k)$, the algebraic group consisting of all $n \times n$ matrices with entries in k and determinant one, and $\mathrm{sl}_n(k)$, the Lie algebra consisting of all $n \times n$ matrices with entries in k and trace zero. Our particular interest lies in representations of $\mathrm{SL}_n(\mathbb{F}_p)$ in the defining characteristic p, i.e., group homomorphisms $\rho : \mathrm{SL}_n(\mathbb{F}_p) \to \mathrm{GL}_m(k)$, or equivalently, linear group actions of $\mathrm{SL}_n(\mathbb{F}_p)$ on an m-dimensional k-vector space V. Such a space V is also referred to as a $\mathrm{SL}_n(\mathbb{F}_p)$-module.

In this setup there are two fundamental questions. What are the irreducible or simple objects? Simple modules are modules that have no non-trivial proper subspaces that are invariant under the group action. These are the smallest building blocks from which other modules can be built. Unlike linear actions of finite groups on finite-dimensional $\mathbb{C}$-vector spaces, where every module is simply a direct sum of simples, modular representation theory allows for more complicated structures to be built out of these smallest building blocks. This leads to the second fundamental question: How and when can we "stick" two simple objects together? This leads to the study of cohomology. The two questions are closely connected. The two mathematicians in the picture below successfully constructed an indecomposable module out of simple objects, each represented by a single piece of lego.



In general the dimensions and characters of the simple $\mathrm{SL}_n(\mathbb{F}_p)$-modules are not known. What we do know is that they are restrictions of a finite subset of the simple objects of the larger algebraic group $\mathrm{SL}_n(k)$ and that the restriction of this same subset to the Lie algebra $\mathrm{sl}_n(k)$ also yields a complete set of simples. Moreover, the cohomology for $\mathrm{SL}_n(\mathbb{F}_p)$ can often be obtained via cohomology data coming from the algebraic group, see for example [2].

One might also ask oneself: How are the representation theories of the groups $\mathrm{SL}_5(\mathbb{F}_{17})$ and $\mathrm{SL}_5(\mathbb{F}_{53})$ related? Is there a general theory that is independent of the underlying prime?

We will concentrate now on the algebraic groups $\mathrm{SL}_n(k)$. As mentioned above, dimensions and characters of the simple modules are in general unknown. There is a second class of modules whose dimensions and characters are known. In some sense these modules, we will refer to them as standard modules, come from the classical representation theory over the complex numbers and the information can easily be obtained via Weyl's well-known character formula. The problem of finding the dimensions of the simple modules is now equivalent to finding the multiplicities of a simple appearing as a composition factor (as a piece of lego) in the larger standard module. Inverting this data leads to expressions of the characters of simple module as $\mathbb{Z}$-linear combinations of the known characters of the standard modules. In 1979 George Lusztig conjectured that, provided the prime is sufficiently large, the coefficients of such a $\mathbb{Z}$-linear combination are given by affine Kazhdan-Lusztig polynomials [6]. As a consequence of this conjecture the behavior would indeed be independent of the underlying prime. For the case of $\mathrm{SL}_n(k)$ Lusztig originally proposed conjecture would result in a bound of $p \geq 2n-3$. Later further evidence was found that suggested his conjecture should hold for all $p > n$.

In 1994 Andersen, Jantzen and Soergel [1] showed that Lusztig's conjecture holds for arbitrarily large primes, without giving any bound on p. The bound $p > n$ had been verified for $n \leq 5$. For larger n the dimensions of the modules and the resulting complexities of the necessary calculations make it virtually impossible to produce more numerical data. Proving Lusztig's conjecture has been the holy grail in modular representation theory for the last 40 years.

Therefore, it came as a shock to the research community when Geordie Williamson announced in 2013 that no linear bound for p in terms of n is sufficient for Lusztig's conjecture to hold [7]. Moreover, he showed that for sufficiently large n one can always produce exponentially large (in terms of n) counterexamples to the expected bounds in Lusztig's conjecture.

The methods developed and applied by Williamson and his collaborators are extremely sophisticated and come from geometric representation theory. Explaining them would go way beyond the scope of this article and way beyond the capabilities of its author. However, in the end the fact that no linear bound exists is a consequence of Carmichael's Theorem and the existence of exponentially large counterexamples to Lusztig's conjecture arise from the fact that a "spider path" of length n will visit exponentially many, exponentially large primes (again in terms of n). For more details we refer the interested reader to [7].

The spider will rest now.

Sittin', thinkin', sinkin', drinkin',
Wondering what I'll do when I'm through tonight.

- Mick Jagger, Keith Richards

References

[1] H.H.Andersen, J.C.Jantzen, W.Soergel. *Representations of quantum at a pth root of unity and of semisimple groups in characteristic p: independence of p*, *Astérisque.* 220 (1994), 321 pp.

[2] C.P.Bendel, D.K.Nakano, C.Pillen. *Extensions for finite Chevalley groups II*, *Trans. Amer. Math. Soc.* 354(11) (2002) 4421–4454.

[3] A.J.Cole, A.J.T.Davie. *A Game Based on the Euclidean Algorithm and a Winning Strategy for It*, *Math. Gaz.* 53 (1969), 354–357.

[4] J.E.Humphreys. *Representations of $SL(2,p)$*, *Amer. Math. Monthly.* 82 (1975), 21–39.

[5] C.Kassel, V.Turaev. *Presentations of $SL_2(\mathbb{Z})$ and $PSL_2(\mathbb{Z})$*, *Braid Groups,* Graduate Texts in Mathematics, vol 247, Springer, New York, NY. (2008), 311–314. https://doi.org/10.1007/978-0-387-68548-9_8

[6] G.Lusztig. *Some problems in the representation theory of finite Chevalley groups*, The Santa Cruz Conference on Finits Groups (Univ. California, Santa Cruz, Calif., 1979), *Proc. Sympos. Pure Math.,* vol. 37, Amer. Math. Soc., Providence, R.I. (1980), 313-317.

[7] G.Williamson. *Schubert calculus and torsion explosion.* With a joint appendix with Alex Kontorovich and Peter J. McNamara. *J. Amer. Math. Soc.* 30(4) (2017) 1023–1046.