PRIMES CIRCLE FINAL REPORT

OLIVIA CHEN AND NATALIE HAN

Abstract. We discuss matrix groups, projective space, projective geometry over a finite field, the math behind Spot It!, and Steiner systems.

1. Introduction

Groups are a type of algebraic structure in abstract algebra with basic properties that give it a wide variety of applications in mathematics and science. For instance, in geometry, groups are essential to understanding projective geometry, which was historically used in the context of art as artists searched for the principles of "projecting" the three-dimensional objects they wanted to depict onto their two-dimensional canvases. Furthermore, the unique properties of groups and projective geometry allow it to model many other interesting scenarios, such as how to design a Spot It! deck. They also can further extend their use even into combinatorics through Steiner systems. In conclusion, although seemingly simple, many complex concepts and situations can be broken down using groups, making them fundamental to many fields of study.

The rest of the paper is organized as follows. Section 2 introduces basic definitions learned throughout the program, including groups, fields, projective spaces, and rings, as well as the game Spot It! Then, section 3 discusses projective space over a finite field, as well as the computations involved, while section 4 discusses Spot It!, which is a game set up about a projective plane over a finite field, and computing the number of cards in a deck. Lastly, Section 5 discusses the steiner system and how it can be used to solve the Kirkman schoolgirl problem.

2. Preliminaries

Definition 1. *A group $\langle G, * \rangle$ is the set G with binary operations and satisfies the following conditions:*

1. *Closure: for all $a, b \in G$, $a * b$ is in G*
2. *Associativity: $(a * b) * c = a * (b * c)$ (for all $a, b, c \in G$)*
3. *Identity: there exists an e so that for all $x \in G$, we have $e * x = x * e = x$*
4. *Inverse: for all $a \in G$ there exists a unique $a' \in G$ so that $a * a' = e$ and $a' * a = e$.*

Definition 2. *The general linear group $\mathrm{GL}(n, \mathbb{R})$ is a group of all $n \times n$ matrices with entries in $\mathbb{R}$ and has a non-zero determinant.*

Definition 3. *The special linear group $\mathrm{SL}(n, \mathbb{R})$ is a group of all $n \times n$ matrices with entries in $\mathbb{R}$ and the determinant being 1.*

Definition 4. *A field F is a ring with special additional properties. It contains binary operations (addition and multiplication) and satisfies the following conditions:*

1. *$\langle F, + \rangle$ is a commutative group*

(2) *$\langle F, * \rangle$ is a commutative group*
(3) *For all $a, b, c \in F$, $a * (b + c) = a * b + a * c$*
(4) *For all $a, b, c \in F$, $(b + c) * a = b * a + c * a$.*

Definition 5. *A finite field is a field that contains a finite number of elements. An example would be $\{0, 1, 2, 3, 4, 5, 6\}$ under mod 7 for addition and multiplication. This works because it satisfies all the properties.*

Spot It! is a card game in which the deck consists of 55 cards, with each card containing 8 symbols, and between any two cards, there is one symbol in common. Each player starts off with one card in their hand, and the remaining cards are stacked in the center. Each turn consists of the players attempting to spot a match between an element in their card and the top card in the stack. If they find a match first, they take the card in the middle as their new card revealing a new card in the middle stack. The goal of the game is to have collected the most cards by the end. This game is secretly quite similar to the other pattern-finding game Set, and the decks for both can be modeled using projective geometry.

Definition 6. *Projective space is the space of all lines going through the origin. Any such line in $\mathbb{R}^n$ can be written as*

$$a_1x_1 + a_2x_2 + ... + a_nx_n = 0$$

which corresponds to the projective point

$$[a_1, a_2, ..., a_n]$$

in $\mathbb{RP}^{n-1}$.

A Euclidean line becomes a projective point, a Euclidean plane becomes a projective line, and so on. In projective space, scalar multiples are equivalent, meaning that $[a_1, a_2, ..., a_n]$ is equivalent to $[ka_1, ka_2, ..., ka_n]$, as $a_1x_1 + a_2x_2 + ... + a_nx_n = 0$ is the same line as $ka_1x_1 + ka_2x_2 + ... + ka_nx_n = 0$.

Projective space in 2 dimensions would be a projective plane, and all of these lines could be written in the form $Ax + By = 0$, where A and B are real numbers. For the rest of this paper, we will be primarily focusing on the projective plane. An especially important property of projective space to the topics in our paper is that any two distinct lines in projective space will intersect at exactly 1 point.

Definition 7. *A ring R is a set with two binary operations, addition (denoted by $a + b$) and multiplication (denoted by ab), such that for all $a, b, c \in R$:*

(1) *$a + b = b + a$,*
(2) *$(a + b) + c = a + (b + c)$,*
(3) *There is an additive identity 0,*
(4) *For $-a$ in R, $(-a) + a = 0$,*
(5) *$a(bc) = (ab)c$,*
(6) *$a(b + c) = ab + ac$ and $(b + c)a = ba + ca$.*

Definition 8. *An ideal I is a subset of the ring's elements such that*

(1) *$(I, +)$ is a subgroup of $(R, +)$,*
(2) *For every $r \in R$ and $x \in I$, we have $rx \in I$.*

Definition 9. *A ring mod an ideal $\mathbb{F}_q[x]/(f(x))$ consists of polynomials with coefficients in field $\mathbb{F}_q$ but replaces all instances of $f(x)$ by 0.*

Example. *$\mathbb{F}_2[x]/(x^2)$ consists of the elements $0, 1, x, x + 1$.*

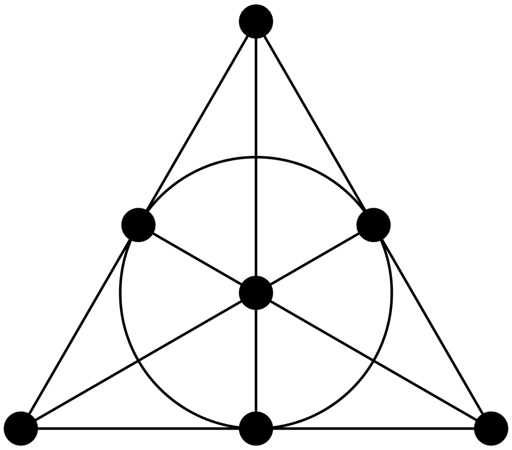

Figure 1. The Fano plane.

3. Finite field geometry

Projective space over a finite field is exactly the same as projective space over $\mathbb{R}$ as described in Definition 6, but replacing $\mathbb{R}$ with $\mathbb{F}_q$ throughout.

The Fano plane is a projective plane containing seven lines, each passing through three points. One such line is a circle. The points here correspond to the non-zero points in the two-dimensional vector space over the finite field of order 2, namely

$$[0:0:1],[0:1:0],[1:0:0],[1:1:0],[1:0:1],[0:1:1],[1:1:1]$$

while the lines correspond to one-dimensional linear subspaces of $\mathbb{F}_2\mathbb{P}^2$.

On a projective line with order n, there are $n+1$ points.

To give some more intuition about projective space, we provide a sample computation. To find the order of $\mathrm{GL}_n(\mathbb{F}_p)$, we are finding the number of invertible $n \times n$ matrices with entries in $\mathbb{F}_p$. In order for a matrix to be invertible, the rows must be linearly independent. Starting from the top row, we find that there are $p^n - 1$ possibilities, as each entry can be one of p options but the whole row cannot all be zeroes. Then, the second row cannot be any multiple of the first row, meaning it has $p^n - n$ possibilities. Generalizing this, for the kth row, there are $p^n - n^{k-1}$ possibilities because the kth row starts with p^n options, but, because it cannot be a linear combination of any of the first $k-1$ rows, eliminating $n^(k-1)$ options. (If we call the rows $r_1, r_2, r_3, ..., r_k - 1$, then all linear combinations of those rows can be written as $a_1r_1 + a_2r_2 + a_3r_3 + ... + a_k - 1r_k - 1$ where every a_i is an integer between 0 and $n-1$.) Therefore, the total number of invertible nxn matrices is $(p^n-1)(p^n-n)...(p^n-n^{n-1})$.

Then, to find the order of $\mathrm{SL}_n(\mathbb{F}_p)$, we are finding the number of $n \times n$ matrices with entries in $\mathbb{F}_p$ that have a determinant of 1. All of these are already included in $\mathrm{GL}_n(\mathbb{F}_p)$. We can find the order of this subgroup through the fact that the ratio of the order of the group to the subgroup is equal to the index of the subgroup and this ratio is $\frac{1}{p-1}$.

The set of projective general or special linear groups can be found from these groups, partitioning them into equivalence classes.

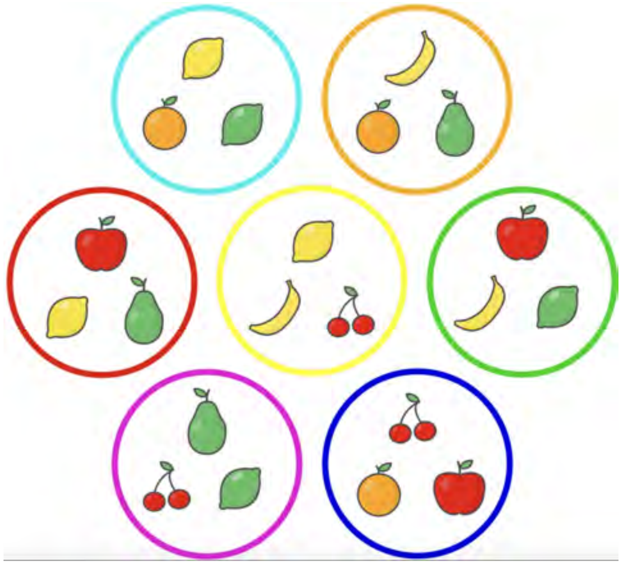

Figure 2. A small Spot It! deck.

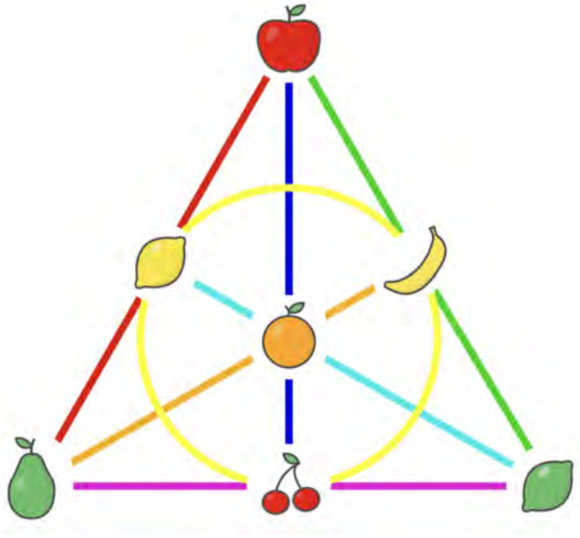

Figure 3. The Fano plane corresponding to this Spot It! deck.

4. Spot It!

As suggested in the introduction, Spot It! may be set up as a game about a projective plane over a finite field. Each card contains a set of symbols that allow us to match up a card with a line in projective space. An example of a small Spot It! deck over the Fano plane is illustrated in Figs 2 and 3.

As we can see, each of the 7 cards corresponds to one of the 7 lines in the Fano plane. Just like any line has 3 points on it, any card has 3 symbols on it. Also, just like any two distinct lines in the Fano plane share exactly 1 point in common, each pair of distinct cards has exactly 1 symbol in common.

The story with the actual Spot It! deck is very similar, except instead of working with the projective plane over $\mathbb{F}_2$ we work over $\mathbb{F}_7$. Each card has 8 symbols on it, just like how each line has 8 points on it. Also, each pair of distinct cards has exactly 1 symbol in common, just like any two distinct lines share exactly 1 point in common. The total number of lines in the projective plane over $\mathbb{F}_p$ is $\frac{p^3-1}{p-1} = p^2+p+1$. So we should expect there to be $7^2+7+1 = 57$ cards in a Spot It! deck. However, there are only 55 cards due to a printing issue. Note also that due to the duality between lines and points in the projective plane, we should expect there to be 57 symbols across all cards in a Spot It! deck. (This is true even after accounting for the two missing cards.)

How can we find the missing two cards? There are lots of ways to do it. One of them is to brute force bash through all of the ways to put 8 of the 57 symbols on a card. But this is not particularly efficient. Another way to do this is to organize the cards by symbol as shown in Figure 4. The bottom row represents the points making up the line at infinity. From this arrangement, we can see the locations of the missing Spot It! cards, and from the lines that pass through each location we can determine relatively easily what the missing Spot It! cards should be. For example, both cards are missing from snowman column so should both have snowmen on them. The cards are:

Ladybug Snowman ! Skull Dog Eye Lightbulb Stop

and

Snowman Dinosaur Person Cactus Maple leaf Ice cube ? Daisy.

5. Steiner systems

Definition 10. *A Steiner system $S(t,k,n)$ is an n-element set X together with a set of k-element subsets ("blocks") so that each t-element subset of X is contained in exactly 1 block.*

The Fano plane is a Steiner system in disguise. In our example of the Fano plane, $X = \{\text{vertices}\}$, blocks are lines, and t-element subsets of X are pairs of points. Any two distinct points lie on a unique line. Three points lie on each line. There are seven points in total. So we have the Steiner system $S(2,3,7)$.

In general, the projective plane is also a Steiner system. A projective plane over $\mathbb{F}_q$ has $\frac{q^3-1}{q-1} = q^2+q+1$ points. Each line passes through $q+1$ points, and each pair of distinct points lies on a unique line. So this plane is a Steiner system $S(2, q+1, q^2+q+1)$. Here, as before, the blocks are lines.

Steiner systems also arise outside of the context of projective space. Here is a famous problem from combinatorics, called Kirkman's schoolgirl problem (1850).

Question 1. 15 *schoolgirls walk in groups of* 3 *each day for* 7 *days. How can they be arranged so that no* 2 *girls walk in the same group more than once?*

There are multiple different solutions to this problem. Here is an example of one. Name the 15 girls A,B,C,...,O.

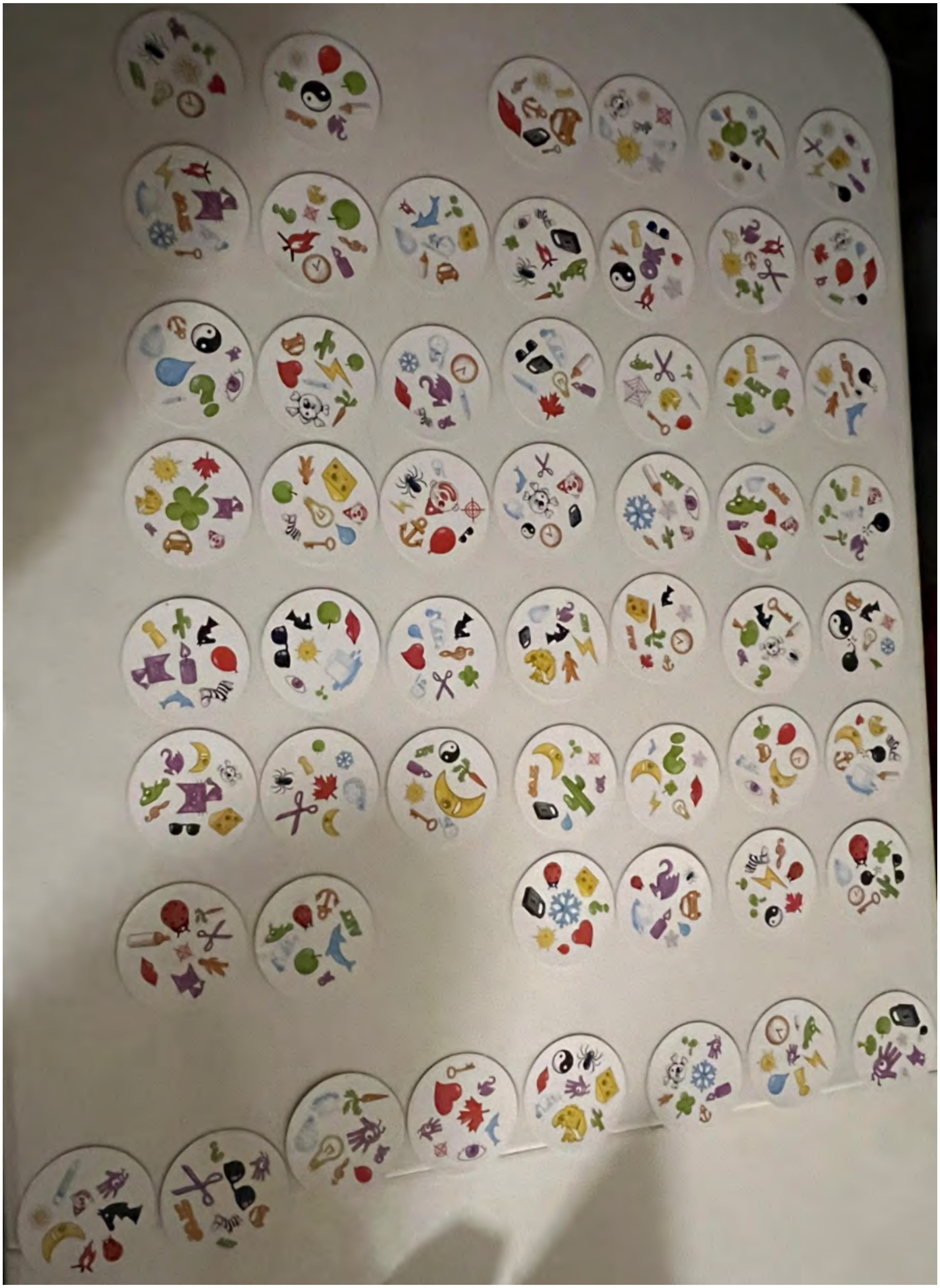

FIGURE 4. the Spot It! cards are arranged like points in the projective plane over $\mathbb{F}_7$. Each line of cards shares exactly one symbol. For example, all the cards in the rightmost column have a bomb.

Table 1: A solution to Kirkman's schoolgirl problem.

Day 1	Day 2	Day 3	Day 4	Day 5	Day 6	Day 7
ABC	ADG	AEO	AIM	AFJ	AHK	ALN
DEF	BEH	BIJ	BDL	BKO	BGN	BFM
GHI	CJM	CDN	CEK	CGL	CFI	CHO
JKL	FKN	FHL	FGO	DHM	DJO	DIK
MNO	ILO	GKM	HJN	EIN	ELM	EGJ

These solutions are examples of $S(2, 3, 15)$ systems.

Given a choice of (t, k, n), one may ask if $S(t, k, n)$ exists. The answer is not known in general, but some specific cases can be handled using abstract algebra.

We describe a smaller version of Kirkman's schoolgirl problem and how we can use some properties of rings to solve it. Our smaller version has 8 girls walking in pairs over 4 days with no repeated pairs. We build $S(2, 2, 8)$ by performing addition over the finite field $\mathbb{F}_4$ as suggested by the below table.

Table 2: A solution to our smaller version of Kirkman's schoolgirl problem.

Day 1	Day 2	Day 3	Day 4
0 0	0 1	0 x	0 $x+1$
1 1	1 0	1 $x+1$	1 x
x x	x $x+1$	x 0	x 1
$x+1$ $x+1$	$x+1$ x	$x+1$ 1	$x+1$ 0

In Table 2, the two values on each day correspond to the pair we're choosing. We perform addition over $\mathbb{F}_4$. On Day 2, we add 1 to all the values. On Day 3, we add x. On Day 4, we add $x + 1$. We do this because 1, x, and $x + 1$ are different elements of $\mathbb{F}_4$. We avoid repeating people since the second person in the pair is rotated each day. We may rewrite Table 2 as

Table 3: A solution to our smaller version of Kirkman's schoolgirl problem, cont.

Day 1	Day 2	Day 3	Day 4
A E	A F	A G	A H
B F	B E	B H	B G
C G	C H	C E	C F
D H	D G	D F	D E

Of course, we could have solved this problem without using group theory via trial and error, or just by cycling the second group of girls on each day. But this approach generalizes more naturally to harder problems, such as the one below, with 24 students walking in rows of 3 for 8 days with no repeated pair. We build $S(2, 3, 24)$. Here we are working over $\mathbb{F}_8 \cong \mathbb{F}_2[x]/(x^3)$.

Table 4: A solution to a bigger version of Kirkman's schoolgirl problem.

Day 1	Day 2	Day 3	Day 4
$0\ 0\ 0$	$0\ 1\ x$	$0\ x\ x^2$	$0\ x+1\ x^2+x$
$1\ 1\ 1$	$1\ 0\ x+1$	$1\ x+1\ x^2+1$	$1\ x\ x^2+x+1$
$x\ x\ x$	$x\ x+1\ 0$	$x\ 0\ x^2+x$	$x\ 1\ x^2$
$x+1\ x+1\ x+1$	$x+1\ x\ 1$	$x+1\ 1\ x^2+x+1$	$x+1\ 0\ x^2+1$
$x^2\ x^2\ x^2$	$x^2\ x^2+1\ x^2+x$	$x^2\ x^2+x\ 0$	$x^2\ x^2+x+1\ x$
$x^2+1\ x^2+1\ x^2+1$	$x^2+1\ x^2\ x^2+x+1$	$x^2+1\ x^2+x+1\ 1$	$x^2+1\ x^2+x\ x+1$
$x^2+x\ x^2+x\ x^2+x$	$x^2+x\ x^2+x+1\ x^2$	$x^2+x\ x^2\ x$	$x^2+x\ x^2+1\ 0$
$x^2+x+1\ x^2+x+1\ x^2+x+1$	$x^2+x+1\ x^2+x\ x^2+1$	$x^2+x+1\ x^2+1\ x+1$	$x^2+x+1\ x^2\ 1$

Table 5: The previous table continued

Day 5	Day 6	Day 7	Day 8
$0\ x^2\ x+1$	$0\ x^2+1\ 1$	$0\ x^2+x\ x^2+x+1$	$0\ x^2+x+1\ x^2+1$
$1\ x^2+1\ x$	$1\ x^2\ 0$	$1\ x^2+x+1\ x^2+x$	$1\ x^2+x\ x^2$
$x\ x^2+x\ 1$	$x\ x^2+x+1\ x+1$	$x\ x^2\ x^2+1$	$x\ x^2+1\ x^2+x+1$
$x+1\ x^2+x+1\ 0$	$x+1\ x^2+x\ x$	$x+1\ x^2+1\ x^2$	$x+1\ x^2\ x^2+x$
$x^2\ 0\ x^2+x+1$	$x^2\ 1\ x^2+1$	$x^2\ x\ x+1$	$x^2\ x+1\ 1$
$x^2+1\ 1\ x^2+x$	$x^2+1\ 0\ x^2$	$x^2+1\ x+1\ x$	$x^2+1\ x\ 0$
$x^2+x\ x\ x^2+1$	$x^2+x\ x+1\ x^2+x+1$	$x^2+x\ 0\ 1$	$x^2+x\ 1\ x+1$
$x^2+x+1\ x+1\ x^2$	$x^2+x+1\ x\ x^2+x$	$x^2+x+1\ 1\ 0$	$x^2+x+1\ 0\ x$

We may rewrite as

Table 6: A solution to a bigger version of Kirkman's schoolgirl problem.

Day 1	Day 2	Day 3	Day 4	Day 5	Day 6	Day 7	Day 8
α Aa	α Bc	α Ce	α Dg	α Ed	α Fb	α Gh	α Hf
β Bb	β Ad	β Df	β Ch	β Fc	β Ea	β Hg	β Ge
γ Cc	γ Da	γ Ag	γ Be	γ Gb	γ Hd	γ Ef	γ Fh
δ Dd	δ Cb	δ Bh	δ Af	δ Ha	δ Gc	δ Fe	δ Eg
ϵ Ee	ϵ Fg	ϵ Ga	ϵ Hc	ϵ Ah	ϵ Bf	ϵ Cd	ϵ Db
ζ Ff	ζ Eh	ζ Hb	ζ Gd	ζ Bg	ζ Ae	ζ Dc	ζ Ca
η Gg	η He	η Ec	η Fa	η Cf	η Dh	η Ab	η Bd
θ Hh	θ Gf	θ Fd	θ Eb	θ De	θ Cg	θ Ba	θ Ac

Here the girls are numbered $\alpha, ..., \theta$, A, ..., H, a, ..., h.

6. Acknowledgments

The authors thank the Primes Circle program, its program coordinators, Mary Stelow and Marisa Gaetz for this opportunity to delve into group theory, and our mentor Katherine Tung for her continuous support throughout the program. They also thank their parents for their encouragement and patience.

7. References

Gallian, *Contemporary Abstract Algebra*.

Mulholland, “SPOT-IT Card Game”, https://www.sfu.ca/~jtmulhol/teaching-musings.html.

Stand-up Maths, “How does Dobble (Spot It!) work?” https://www.youtube.com/watch?v=VTDKqW_GLkw.

“Finite Projective Planes and the Math of Spot It!” https://puzzlewocky.com/games/the-math-of-spot-it/.