

HARMONY AMID CHAOS

Measuring the Randomness of Galois Fields

Drew Morgan Schaffner

Faculty Mentor: Dr. Justin Brown

Abstract

We provide a brief but intuitive study on the subjects from which Galois Fields have emerged and split our study up into two categories: harmony and chaos. Specifically, we study finite fields with p^2 elements where p is prime. Such a finite field can be defined through a $p \times p$ logarithm table. The Harmony Section is where we provide three proofs about the overall symmetry and structure of the Galois Field as well as several observations about the order within a given table. In the Chaos Section we make two attempts to analyze the tables, the first by methods used by Vladimir Arnold as well as (what we believe is) an improvement of his method, the second by statistical analysis of the Galois Fields at $p = 17$, the highest prime value we were able to generate Galois Fields of size p^2 for.

INTRODUCTION

A Galois Field is a field with a finite number of elements, which belongs to a subset of “the most fundamental mathematical objects” and supplies a foundation for “all other mathematical structures and models” (Arnold, 2011, p. 1).

Perhaps the best place to begin is with an easily understood, but nonetheless complex, mathematical object, the prime numbers:

$$p = 2, 3, 5, \dots;$$

which of course form that set of integers greater than zero which only have two divisors (these being 1 and p). But much lesser known than the prime numbers are the set of elements which form what is known as a field.

A field is closed under the operations of addition and multiplication (with associative, commutative, and distributive properties) such that every element has an additive inverse and every nonzero element has a multiplicative inverse.

Consider a prime number, p ; a field can be formed by the residues modulo p . For instance, the simplest field, $p = 2$. I should like to introduce the notation $GF(p)$, taking $p = 2$, to mean the field

$$\mathbb{Z}/2\mathbb{Z} = \{0, 1\}.$$

A simple check ensures that this set is closed under addition and multiplication and contains the inverses it needs (note that since we are adding and multiplying elements of $\mathbb{Z}/2\mathbb{Z}$, the operations will be closed):

$$\begin{aligned} 0 + 0 &= 0, & 0 + 1 &= 1, & 1 + 1 &= 0, \\ 0 \cdot 0 &= 0, & 0 \cdot 1 &= 0, & 1 \cdot 0 &= 0, & 1 \cdot 1 &= 1. \end{aligned}$$

Therefore, $GF(2)$ is a field. A similar example and proof can be made for $GF(3)$ using the same method above. With $GF(4)$, however, a more tactile approach is needed.

If $\mathbb{Z}/4\mathbb{Z} = \{0, 1, 2, 3\}$ then the number 2 has no inverse, since the residues of $2x$ equal 0 or 2. This alone seems to imply that a field with four elements does not exist. But they do; enter the finite field.

Such fields were first introduced in the 1800s by a young mathematician named Évariste Galois. They are part of a subset of fields that are finite and are given the name Galois Fields to honor their creator. Two theorems about finite fields have a direct influence on our study:

1. The number of elements within a finite field is a prime number, p , raised to some natural number n .
2. For every such p^n there is a field with p^n elements, and any two fields with p^n elements are isomorphic.

In other words, the notation we introduced above is not precise enough to exhaust the set of finite fields. We shall take $GF(p^n)$ to mean the Galois Field with p^n elements (Arnold, 2011, p. 6).

To form a Galois Field with p^2 elements we must consider each element in the field as a linear combination of A 's and 1 's:

$$GF(p^2) = \{x \mid x = \alpha A + \beta, \text{ s.t. } 0 \leq \alpha \leq p-1 \text{ and } 0 \leq \beta \leq p-1\}.$$

Using this method, it becomes rather easy to generate every single element in a field up to and including additive and multiplicative identities, but it does not give us a good way of telling whether the field is cyclic; in other words, this method tells us almost nothing about the structure of a field. For that, a method of defining the elements must be generated. Take $GF(2^2)$ into consideration.

Exhausting all possible combinations of α and β yields the following set:

$$GF(2^2) = \{0, 1, A, A+1\};$$

it may not exactly be clear that this is a field, but the simple test applied above can still be applied:

$$\begin{aligned} 0+0 &= 0, & 0+1 &= 1, & 0+A &= A, & 0+(A+1) &= A+1, \\ 1+1 &= 0, & 1+A &= A+1, & 1+(A+1) &= A, \\ A+A &= 0, & A+(A+1) &= 1, \\ (A+1)+(A+1) &= 0, \\ 0 \cdot 0 &= 0, & 0 \cdot 1 &= 0, & 0 \cdot A &= 0, & 0 \cdot (A+1) &= 0, \\ 1 \cdot 1 &= 1, & 1 \cdot A &= A, & 1 \cdot (A+1) &= A+1, \\ A \cdot A &= A^2, & A \cdot (A+1) &= A^2 + A, \\ (A+1) \cdot (A+1) &= A^2 + 1. \end{aligned}$$

And here we run into an issue that, on initial inspection, appears to show that $GF(2^2)$ is not a field: you will notice that A^2 , $A^2 + A$ and $A^2 + 1$ were not elements in our initial set. However, what we are really beginning to see is that these Galois Fields are behaving much like the imaginary numbers that we are so used to. “ $i^2 = -1$ ” is notorious; it is in effect saying, “The square root of negative one does not exist, therefore, let us create this strange value, i , such that $\sqrt{-1} = i$.” It causes us no pause; we are very used to this strange redefinition of an abstract value. And so, it should cause us no pause here: suppose that $A^2 = A+1$, what then?

$$\begin{aligned} A \cdot A &= A^2 = A+1, & A \cdot (A+1) &= A^2 + A = A+1+A=1, \\ (A+1) \cdot (A+1) &= A^2 + 1 = A+1+1=A. \end{aligned}$$

The problem is alleviated; as we can see, the field is still closed, none of the elements are outside the initial set, and every element has an additive inverse and every nonzero element a multiplicative inverse. You may object to our definition of A^2 , noticing the choice is arbitrary. However, if we were to choose $A^2 = A$, issues would have arisen. For instance, $A \cdot (A+1) = A^2 + A = 0$, so neither A nor $A+1$ could have a multiplicative inverse. This is a reasonable objection, but it simply means that $A^2 = A+1$ is a far superior choice (in later sections we will go into detail about how to select A^2).

This may seem insignificant, but it has allowed us also to redefine $GF(2^2)$ as the powers of A :

$$\begin{aligned} A^2 &= A+1, \\ A^3 &= A^2 + A = A+1+A=1, \\ A^4 &= A. \end{aligned}$$

Therefore, as an expression of the powers of A , $GF(2^2) = \{0, A, A^2, A^3\} = \{0, A, A + 1, 1\}$; respectively.

In sum, by defining A^2 we have defined the cyclic group in $GF(2^2)$. And in general (for $GF(p^2)$) we can define these fields with a single recursive operation.

Given a proper choice of $A^2 = \alpha A + \beta$, such that α and β are “good” choices, we can express the values of A^k , where $k \leq p^2 - 1$, as the expression

$$A^k = v_k \cdot A + u_k \cdot 1, \quad \text{where } v_{k+1} = \alpha v_k + u_k \quad \text{and} \quad u_{k+1} = \beta v_k.$$

Using this method, we can generate $GF(2^2)$ as before, but without the hassle of performing algebraic operations (if you like, we recommend trying this out by hand; it may help the reader grasp the operation). This method may seem inferior when dealing with a field with only four elements, but when performing higher order operations during which code will be implemented, the formula is superior.

And it is in this manner that we shall bridge into the topic of this paper, the formulation of the Galois Table, a visual representation of the Galois Field.

The last field we generated was quite simple with only four elements, expressed as $GF(2^2) = \{0, A, A^2, A^3\} = \{0, A, A + 1, 1\}$, perhaps more clearly as

$$0 = 0, \quad A = A, \quad A^2 = A + 1, \quad A^3 = 1.$$

Consider the table expressing the powers on A^k akin to a table of logarithms, whereby the elements inside the table represent the power on A and the indices represent the values (u_k, v_k) : the column is u_k and the row is v_k .

1	1	2
0	∞	3
	0	1

Figure 1: The Galois Table of $GF(2^2)$ with $A^2 = A + 1$.

The use of the infinity symbol is based on $\log(0) = -\infty$: no power of A is ever 0, so the cell for $0 = 0 \cdot A + 0$ holds no exponent. We write ∞ without a sign, since the elements of a finite field are neither positive nor negative.

Now, choosing the Galois Field from $p = 2$ is not difficult, as there is only one choice for what A^2 should equal, but for succeeding prime numbers the number of possible fields (choices for α and β) grows. We wrote code to aid in testing the number of possible logarithm tables for primes under 200; this is a sampling of our data:

p	Number of $GF(p^2)$
2	1
5	4
7	8
17	48
29	96
53	432
89	960
137	2816
173	4704
199	4800

As the reader can see, the number of tables grows quickly as p increases. We should note the methodology used to generate tables and why certain values for α and β are not as “good” as others.

Let $p = 7$, and suppose that we have used the recursive formulas defined above and a simple nested for loop to generate all possible combinations where $A^2 = \alpha A + \beta$. Note, there are (by combinations) $7^2 = 49$ unique combinations for α and β . But, if the reader will look back at the number of possible Galois Fields, they will notice that there are only 8. How are we to separate the 41 “bad” choices from the 8 “good” choices?

Using code, this can be done with Boolean operators. We can use the number of nonzero elements in the field, $p^2 - 1$, to fix the number of unique elements the recursion must generate: if the recursive formula and the choice of α and β generate unique values for the first $p^2 - 1$ (in this case 48) powers, then we keep the table (include it as one of the 8). If, however, the recursive formula and the choice for α and β repeats before cycling through all 48 nonzero elements, then we throw away the table (exclude it from the set of 8).

But this provides no theoretical mathematical framework on which we can judge a table based on the choice of A^2 as good or bad. The method we used beforehand simply iterates the recursive formula 48 times with a particular α and β , and tells whether it should be included or excluded based on the uniqueness of the elements produced in the string with length 48. But say I were to give the reader $A^2 = \alpha A + \beta$: what then? Could the reader tell whether it was “good” or “bad” (included or excluded)?

Of course, one could, by hand or by code, repeat the process described above (by hand it would be quite tedious for a large prime number). But if we did not want to go to all that work, or if we did not know how to write code, one of the ways we could tell is whether the equation

$$A^2 - \alpha A - \beta = 0$$

(formed by setting $A^2 = \alpha A + \beta$ equal to zero) has no integer solutions mod p . If it has a solution c , then $A^2 - \alpha A - \beta = (A - c)(A - c')$ factors, the product of two nonzero elements can be zero, and no field arises; so “good” choices are always among those with no integer solutions.

Notice that this test only rules choices out. There are instances where a choice has no integer solutions but does not generate the table. For instance, in $p = 5$, there are 4 sets of α and β that generate the whole field of 25 elements; using code these have been identified:

$$A^2 \in \{2A + 2, 3A + 2, A + 3, 4A + 3\}.$$

If you set each of these equal to zero, you will find that they have no integer solutions, but you can draw out all the possible combinations for α and β and you will find that there are 6 other choices for A^2 that have no integer solutions. But this is a great improvement given our knowledge of how many possible combinations there are for α and β . In $p = 5$ there are 25 combinations; excluding those with integer solutions, there are 10, only 4 of which end up generating the whole set (those being the ones above).

What separates the two is the order of A . When $A^2 - \alpha A - \beta$ has no integer solutions, the elements $\alpha A + \beta$ form the field $GF(p^2)$, and its nonzero elements form a cyclic group of order $p^2 - 1$; but A itself may have smaller order, and then its powers repeat early. A choice is “good” exactly when A has order $p^2 - 1$, that is, when $A^2 - \alpha A - \beta$ is what is called a *primitive polynomial*. This also explains the counts in the table above: the cyclic group has $\varphi(p^2 - 1)$ generators, where φ is Euler’s totient function, and each good choice of A^2 is satisfied by exactly two of them (A and A^p), so there are

$$\frac{\varphi(p^2 - 1)}{2}$$

Galois Tables of $GF(p^2)$ (Lidl & Niederreiter, 1997, ch. 3). For $p = 7$ this is $\varphi(48)/2 = 8$.

In sum, we can rid ourselves of the brute force method of iterating every single combination for α and β to see if the table is filled, and decrease the number of iterations that the program would need to run through.

Using these rules, it is possible to generate tables with an even greater number of elements; the largest tables we generated were from $p = 17$. In bright green we have highlighted all the prime numbers in the set, and in

yellow, we have highlighted the arms of the diagonals (the cells with $u = v$ or $u = -v$, where a prime keeps its green). This has been done to note the “twinness” of two tables, which we originally defined using the diagonal arms of the table and the prime numbers within. Below are two twins from $p = 17$, for $A^2 = 4A + 3$ and $A^2 = 13A + 3$, although the reader should note that there are 48 total tables using our method of generation.

16	145	191	171	223	17	78	194	208	149	106	87	183	218	85	224	274	30
15	109	70	155	51	135	147	187	182	269	49	42	188	158	238	172	282	113
14	19	68	92	65	82	247	45	23	98	97	268	148	179	249	192	240	57
13	73	13	34	6	119	152	15	122	99	202	111	136	151	246	146	77	233
12	91	154	170	251	129	137	95	220	24	164	117	52	264	140	31	169	33
11	271	61	32	232	56	112	29	143	46	213	211	156	9	204	275	21	62
10	199	132	141	40	277	203	139	245	248	237	84	71	160	278	225	262	272
9	37	166	265	75	286	100	258	115	83	210	116	110	267	41	86	197	63
8	181	207	53	230	185	123	254	260	66	227	259	114	244	142	219	121	22
7	55	128	118	81	134	16	215	228	93	104	101	283	59	133	184	285	276
6	127	206	165	131	60	153	12	67	69	190	287	173	256	200	88	176	205
5	235	177	25	175	284	120	196	261	20	168	76	239	281	273	107	26	10
4	217	89	221	2	102	7	280	255	58	243	266	159	8	263	150	178	157
3	163	201	96	48	105	35	4	124	241	242	167	189	103	226	209	236	212
2	253	257	138	28	94	14	44	186	193	125	38	43	3	279	195	11	214
1	1	174	130	80	229	74	39	231	250	5	64	50	222	161	79	27	47
0	∞	288	252	162	216	234	126	54	180	36	198	270	90	72	18	108	144
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16

Figure 2: The Galois Table of $GF(17^2)$ for $A^2 = 4A + 3$.

16	145	174	130	80	85	74	183	87	250	149	64	50	222	17	223	171	191
15	109	113	138	28	94	14	44	186	49	269	38	187	147	135	51	155	214
14	19	57	96	48	249	179	4	124	97	242	23	45	247	226	65	236	212
13	73	233	77	2	102	151	280	111	58	99	266	15	8	119	150	178	13
12	91	33	169	31	284	120	196	117	20	168	76	95	137	129	251	26	10
11	271	206	21	275	60	9	12	211	213	190	143	29	256	200	88	176	61
10	199	128	118	225	134	16	71	228	237	104	245	139	203	277	184	141	276
9	37	63	197	230	41	267	254	260	66	83	115	114	244	142	75	265	22
8	181	166	121	219	286	100	258	259	227	210	116	110	123	185	86	53	207
7	55	132	285	40	133	59	283	101	248	93	84	215	160	278	81	262	272
6	127	205	32	232	56	112	173	287	46	69	67	156	153	204	131	165	62
5	235	154	170	107	273	281	239	220	24	164	261	52	264	140	175	25	177
4	217	157	34	6	263	152	159	122	243	202	255	136	7	246	146	221	89
3	163	68	92	209	82	103	189	167	98	241	268	148	35	105	192	240	201
2	253	70	11	195	279	3	43	182	125	193	42	188	158	238	172	282	257
1	1	47	27	79	161	78	194	208	5	106	231	39	218	229	224	274	30
0	∞	288	252	162	216	234	126	54	180	36	198	270	90	72	18	108	144
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16

Figure 3: Its twin, the Galois Table for $A^2 = 13A + 3$.

Spend some time gleaning through these two tables, and you will no doubt come to notice two properties.

The first is the “center” of the table. If you have not noticed this, look in the very middle of the diagonal, and subtract elements opposite from one another. So, in Figure 2, subtract $210 - 66 = 144$ or $227 - 83 = 144$. This property is reliant on the entry $(17 - 1, 0)$ where $n = 144$, and can be proven simply for all odd p .

In general, the bottom right corner of the Galois Table is always $\frac{1}{2}(p^2 - 1)$. Let $x = \frac{1}{2}(p^2 - 1)$. Then $(A^x)^2 = A^{p^2-1} = 1$, and the only square roots of 1 in a field are 1 and -1 ; since the powers of A do not repeat before A^{p^2-1} , $A^x \neq 1$, and so $A^x = -1 = 0 \cdot A + (p - 1)$. And thereby, if we suppose there is some value a where A^a is defined by the table, multiplying A^a by A^x yields $-A^a$, and it is precisely this that produces the symmetry defined above: the cells (u, v) and $(-u, -v)$, which (for $u, v \neq 0$) sit opposite one another about the center, hold exponents differing by $\frac{1}{2}(p^2 - 1)$ modulo $p^2 - 1$.

The second property is a little more important in the scheme of our study, which is the difference between two tables, and in general, the twins have a sort of symmetry about each other. The twin of the table for $A^2 = \alpha A + \beta$ is the table for $A^2 = -\alpha A + \beta$. The arms of the diagonal rotate about one another when looking between the two tables. The odd values flip across a vertical line through the center of the diagonal, and the even values flip across a similar horizontal line: an odd exponent in cell (u, v) of one table sits in cell $(-u, v)$ of its twin, and an even exponent in cell (u, v) sits in cell $(u, -v)$. (This is Theorem 2 below.) We have included

two smaller tables for the reader to examine the property more closely:

12	85	7	13	158	59	40	75	8	20	51	100	11	122
11	71	162	161	6	167	37	144	86	45	165	26	108	61
10	29	163	152	119	44	19	125	123	120	102	66	132	3
9	57	72	148	31	147	151	160	12	153	94	23	47	130
8	127	62	32	53	117	49	93	101	164	50	55	142	82
7	15	109	149	106	138	88	105	52	30	118	5	157	111
6	99	27	73	89	34	114	136	21	4	54	22	65	25
5	43	166	58	139	134	80	17	9	133	33	137	116	146
4	141	46	131	107	10	69	96	76	67	63	115	64	156
3	113	87	48	150	18	36	39	41	103	128	35	68	79
2	155	145	24	110	81	129	2	60	121	83	90	77	78
1	1	38	95	16	135	104	92	159	124	143	74	97	91
0	∞	168	154	112	140	42	98	14	126	56	28	70	84
	0	1	2	3	4	5	6	7	8	9	10	11	12

12	85	38	11	16	51	104	92	75	124	59	74	13	7
11	71	61	24	110	165	45	2	60	37	167	90	161	78
10	29	3	48	150	18	36	123	125	19	128	119	68	163
9	57	46	47	23	10	153	96	76	151	147	31	64	156
8	127	166	58	55	134	80	101	93	49	117	53	116	146
7	15	111	157	5	34	114	136	105	4	54	22	149	109
6	99	25	65	106	138	88	21	52	30	118	89	73	27
5	43	62	32	137	33	133	9	17	164	50	139	142	82
4	141	72	148	115	63	67	160	12	69	94	107	131	130
3	113	79	152	35	44	103	41	39	120	102	66	132	87
2	155	162	77	6	83	121	144	86	129	81	26	108	145
1	1	91	97	158	143	40	159	8	20	135	100	95	122
0	∞	168	154	112	140	42	98	14	126	56	28	70	84
	0	1	2	3	4	5	6	7	8	9	10	11	12

Figure 4: Twins in $GF(13^2)$: $A^2 = 2A + 6$ and $A^2 = 11A + 6$. The red dot marks the center, where the diagonals cross.

Now that the reader has (hopefully) a much clearer grasp of the Galois Fields, we can begin to understand that there are two sorts of emerging categories: one that is ordered, harmony, and another that is far less understood and perhaps more interesting, the property of randomness, chaos.

HARMONY

This is a section that is composed of proofs and helps tell us more about the overall harmony within Galois Tables. Throughout, p is an odd prime; for $p = 2$ there is only one table, and $-A = A$.

THEOREM I. *If $A_i^2 = \alpha A_i + \beta$ has no integer solutions mod p , then $A_k^2 = -\alpha A_k + \beta$ has no integer solutions mod p .*

PROOF. Let $A_i^2 = \alpha A_i + \beta$. We take this to mean that $A_i^2 - \alpha A_i - \beta$ has no integer factors for α and β ; such a factorization would imply that A_i^2 is not a “good” choice for A^2 .

Suppose for contradiction that $A_k^2 = -\alpha A_k + \beta$ where A_k^2 has integer factors, which means it is not a “good” choice for A^2 . Set it equal to zero, such that

$$A_k^2 + \alpha A_k - \beta = (A_k + c_1)(A_k + c_2) = 0,$$

where $-\beta = c_1 c_2$ and $\alpha = c_1 + c_2$ for some $c_1, c_2 \in \mathbb{Z}/p\mathbb{Z}$.

Now set $A_i^2 = \alpha A_i + \beta$ equal to zero and attempt to find integer solutions based on the factors of A_k^2 . Taking the negatives of c_1 and c_2 , their sum is $-\alpha$ and their product is still $-\beta$, so

$$(A_i - c_1)(A_i - c_2) = A_i^2 - (c_1 + c_2)A_i + c_1 c_2 = A_i^2 - \alpha A_i - \beta,$$

and $A_i^2 - \alpha A_i - \beta = 0$ has the integer solutions c_1 and c_2 : a contradiction, since it has no integer solutions.

Therefore, by contradiction, if $A_i^2 - \alpha A_i - \beta$ has no integer solutions mod p , neither does $A_k^2 + \alpha A_k - \beta$. ■

THEOREM 2. *If $A_1^n = \alpha' A_1 + \beta'$, $A_1^2 = \alpha A_1 + \beta$ and $A_2^2 = -\alpha A_2 + \beta$, then there is a table where $A_2^n = -\alpha' A_2 + \beta'$ if n is even and $A_2^n = \alpha' A_2 - \beta'$ if n is odd.*

Proof by cases. Suppose that $A_1^n = \alpha' A_1 + \beta'$, and let $A_1^2 = \alpha A_1 + \beta$. Put $A_2 = -A_1$. Then

$$A_2^2 = A_1^2 = \alpha A_1 + \beta = -\alpha A_2 + \beta,$$

so A_2 satisfies $A_2^2 = -\alpha A_2 + \beta$, and its powers make the table for that choice. Since $A_2^n = (-1)^n A_1^n$:

First case, n is even:

$$A_2^n = A_1^n = \alpha' A_1 + \beta' = -\alpha' A_2 + \beta'.$$

Second case, n is odd:

$$A_2^n = -A_1^n = -\alpha' A_1 - \beta' = \alpha' A_2 - \beta'.$$

Therefore there is a table where $A_2^n = -\alpha' A_2 + \beta'$ if n is even and $A_2^n = \alpha' A_2 - \beta'$ if n is odd. ■

THEOREM 3. *Suppose that $A_1^2 = \alpha A_1 + \beta$ and $A_2^2 = -\alpha A_2 + \beta$. If the powers on A_1 generate the Galois Field with p^2 elements, $\{A_1, A_1^2, A_1^3, \dots, A_1^{p^2-1}\}$ where $A_1^{p^2-1} = 1$, then the powers on A_2 also generate the Galois Field with p^2 elements.*

PROOF. As in the proof of **Theorem 2**, let $A_2 = -A_1$, and let $A_1^{p^2-1} = 1$ with no earlier power of A_1 equal to 1.

Suppose for contradiction that $A_2^i = 1$ for some $0 < i < p^2 - 1$, meaning that the succeeding powers on A_2 repeat elements before wrapping all the way through the nonzero elements of $GF(p^2)$. Since $A_2^i = (-1)^i A_1^i$, we split into two cases.

Odd case: suppose i is odd. Then $A_1^i = -A_2^i = -1$. We showed above that $A_1^x = -1$ for $x = \frac{1}{2}(p^2 - 1)$, and the powers of A_1 below $p^2 - 1$ are all different, so $i = x$. But $p^2 - 1 = (p - 1)(p + 1)$ is a product of two consecutive even integers, one of which is divisible by 4, so $p^2 - 1$ is divisible by 8 and x is even. This is a contradiction, since i is odd.

Even case: suppose i is even. Then $A_1^i = A_2^i = 1$ with $0 < i < p^2 - 1$. This is a contradiction, since no power of A_1 before the $(p^2 - 1)$ th equals 1.

Therefore, by cases, if the powers on A_1 generate the Galois Field with p^2 elements, then the powers on A_2 also generate the Galois Field with p^2 elements. ■

Together, **Theorems 1** and **3** say that every table has a twin: if $A^2 = \alpha A + \beta$ is a good choice then so is $A^2 = -\alpha A + \beta$, and **Theorem 2** tells us exactly how the two tables are related.

CHAOS

This section is a little more difficult to lay out. Firstly, what do we mean by chaos? Is the nonappearance of order the defining hallmark of chaos? Is the fact that we cannot identify a discernible structure evidence that there is some sort of underlying structure which we are unable to identify, or evidence of no structure whatsoever? These are all very confusing questions, and one of the ways that we have attempted to address them is through coming up with our own method, which is a little different from the method described by Vladimir Arnold.

Arnold's Conjecture for Equidistribution

The Arnold Method for determining uniformity or equidistribution of a Galois Table relies on dividing the table through a vertical line (which we get to choose); this allows us to specify two areas, the total area, which we shall call z , and the subdivided area, which we shall call G . The fraction G/z yields the proportion of cells in the section. Then we shall take N to mean the number of values in the Galois Table less than a value m which occur in the region G . Then the fraction N/m is the proportion of N to the value of m (Arnold, 2011, p. 17).

Arnold proposes:

$$\lim_{p \rightarrow \infty} \frac{N}{m} = \frac{G}{z}$$

(Arnold, 2011, p. 19). And as far as we can tell, this conjecture appears to be true. But his method is only concerned with single tables; during this project, we became more concerned with the variations of all the tables within a field. That is, how does this limit vary with respect to all the choices of α and β ? We have formed a simple table showing this for $p = 17$ which uses $m = 145$ in every table and utilizes the first seven columns to divide the table into $G = 119$ and $z = 289$. Here is the collected data using Arnold's Method.

Note that the coordinates represent all of the possible choices of β and α , and the resulting $|Arnold| = |N/m - G/z|$ is taken by subtracting one side of the equation from the other and then taking the absolute value.

(β, α)	$ Arnold $	(β, α)	$ Arnold $
(3, 4)	0.057200811	(10, 1)	0.004868154
(3, 6)	0.025557809	(10, 4)	0.022718053
(3, 7)	0.032454361	(10, 5)	0.029614604
(3, 10)	0.036511156	(10, 12)	0.039350913
(3, 11)	0.029614604	(10, 13)	0.008924949
(3, 13)	0.029614604	(10, 16)	0.046247465
(5, 2)	0.018661258	(11, 2)	0.060040568
(5, 3)	0.011764706	(11, 6)	0.036511156
(5, 5)	0.002028398	(11, 8)	0.039350913
(5, 12)	0.025557809	(11, 9)	0.015821501
(5, 14)	0.039350913	(11, 11)	0.050304260
(5, 15)	0.008924949	(11, 15)	0.018661258
(6, 2)	0.029614604	(12, 3)	0.002028398
(6, 7)	0.057200811	(12, 5)	0.022718053
(6, 8)	0.015821501	(12, 8)	0.008924949
(6, 9)	0.002028398	(12, 9)	0.032454361
(6, 10)	0.015821501	(12, 12)	0.004868154
(6, 15)	0.011764706	(12, 14)	0.015821501
(7, 1)	0.002028398	(14, 1)	0.011764706
(7, 3)	0.004868154	(14, 6)	0.087626775
(7, 4)	0.004868154	(14, 7)	0.060040568
(7, 13)	0.060040568	(14, 10)	0.022718053
(7, 14)	0.008924949	(14, 11)	0.004868154
(7, 16)	0.011764706	(14, 16)	0.057200811

As you can see, the results are quite close to zero, but there is one issue: the area we have taken into consideration, shown below using a table from $p = 13$, contains a flaw under Arnold's Method. This region contains a part of the table which has relative symmetry. This being the diagonals, it would not be an issue if it took only one of the diagonals into consideration, but it does not; as I have outlined a hypothetical area G in blue below, we can clearly see that both diagonals are included in the calculation:

12	85	105	13	16	60	51	106	101	53	118	75	24	124
11	155	3	7	123	83	20	86	145	130	94	121	26	8
10	29	62	163	49	19	50	125	136	45	128	68	165	4
9	57	47	73	32	77	164	25	23	153	96	90	78	156
8	43	11	142	150	64	63	76	18	82	59	139	33	9
7	99	38	132	115	65	30	119	138	89	67	120	74	27
6	15	111	158	36	151	5	54	35	114	149	31	48	122
5	127	93	117	55	143	166	102	160	147	148	66	58	95
4	141	72	162	6	12	69	107	109	80	161	116	157	131
3	113	88	81	152	44	129	52	41	134	103	133	79	146
2	71	92	110	37	10	46	61	2	104	167	39	91	87
1	1	40	108	159	34	137	17	22	135	144	100	97	21
0	∞	168	70	112	140	126	14	98	42	56	28	154	84
	0	1	2	3	4	5	6	7	8	9	10	11	12

Figure 5: A region for Arnold's Method in the table for $A^2 = 2A + 7$ in $GF(13^2)$: the first five columns.

Now to a new observer of these fields, this may not seem to be a large issue, but one must understand that every single table has a twin, and these are identified by the difference between the diagonals (defined at the beginning). So, we can see that at least the most visible symmetry occurs between the diagonals, and then too that if one diagonal possesses even numbers, the other possesses odd values. We argue that this “ruins” the calculation which Arnold proposes to identify the randomness of a table and that if we define a new area, it would be possible to obtain values even closer to zero. So, to solve this issue, we propose a new method, the Morgan Method.

Morgan's Conjecture for Equidistribution

Following on the tail of Arnold's Method, the same values will be used, but the area of the table under consideration for uniformity will be slightly different. We will still be comparing the proportion G/z to the proportion N/m , and their meanings will be the same as above. However, for our area we will be more rigid, always taking into consideration the following area across all tables, under all values of p :

12	85	7	13	158	59	40	75	8	20	51	100	11	122
11	71	162	161	6	167	37	144	86	45	165	26	108	61
10	29	163	152	119	44	19	125	123	120	102	66	132	3
9	57	72	148	31	147	151	160	12	153	94	23	47	130
8	127	62	32	53	117	49	93	101	164	50	55	142	82
7	15	109	149	106	138	88	105	52	30	118	5	157	111
6	99	27	73	89	34	114	136	21	4	54	22	65	25
5	43	166	58	139	134	80	17	9	133	33	137	116	146
4	141	46	131	107	10	69	96	76	67	63	115	64	156
3	113	87	48	150	18	36	39	41	103	128	35	68	79
2	155	145	24	110	81	129	2	60	121	83	90	77	78
1	1	38	95	16	135	104	92	159	124	143	74	97	91
0	∞	168	154	112	140	42	98	14	126	56	28	70	84
	0	1	2	3	4	5	6	7	8	9	10	11	12

Figure 6: The region for the Morgan Method in the table for $A^2 = 2A + 6$ in $GF(13^2)$.

The values under the triangle and inside it: the area of values enclosed inside the arms of the top two diagonals, excluding the diagonal on the right side. Precisely, these are the cells (u, v) in the rows $v > \frac{1}{2}(p-1)$ with $p-v \leq u < v$. All in all, there are 36 values, a constant across all tables in $p = 13$, and an easy way to make the area under consideration uniform for different values of p ; in general there are $(\frac{p-1}{2})^2$.

Using $G = 64$, under $p = 17$, therefore $z = 289$, and for m we will still use 145, so we can compare the two methods later on. N , per the definition in Arnold's Method, will be counted within the new area. Doing so, we obtain the following.

(β, α)	$ Morgan $	(β, α)	$ Morgan $
(3, 4)	0.014556735	(10, 1)	0.019926023
(3, 6)	0.019926023	(10, 4)	0.006132920
(3, 7)	0.007660184	(10, 5)	0.013029471
(3, 10)	0.000763632	(10, 12)	0.006132920
(3, 11)	0.006132920	(10, 13)	0.006132920
(3, 13)	0.040615678	(10, 16)	0.000763632
(5, 2)	0.013029471	(11, 2)	0.055936046
(5, 3)	0.035246391	(11, 6)	0.019926023
(5, 5)	0.006132920	(11, 8)	0.035246391
(5, 12)	0.019926023	(11, 9)	0.061305333
(5, 14)	0.000763632	(11, 11)	0.075098437
(5, 15)	0.019926023	(11, 15)	0.019926023
(6, 2)	0.040615678	(12, 3)	0.026822575
(6, 7)	0.040615678	(12, 5)	0.033719127
(6, 8)	0.054408782	(12, 8)	0.013029471
(6, 9)	0.021453287	(12, 9)	0.006132920
(6, 10)	0.026822575	(12, 12)	0.014556735
(6, 15)	0.000763632	(12, 14)	0.014556735
(7, 1)	0.007660184	(14, 1)	0.013029471
(7, 3)	0.007660184	(14, 6)	0.062832598
(7, 4)	0.028349839	(14, 7)	0.042142942
(7, 13)	0.006132920	(14, 10)	0.026822575
(7, 14)	0.013029471	(14, 11)	0.028349839
(7, 16)	0.006132920	(14, 16)	0.040615678

Is the Morgan Method better than the Arnold Method; that is, does our limit approach zero better than his? Difficult to say; we can only do two things to compare the two methods. The first is statistical: compare the averages, standard deviations, as well as the maximum and minimum value of the methods. The second is a simple difference between each table under both methods using the coordinates of α and β .

Statistical.

	Arnold	Morgan
Average	0.025946586	0.022510241
Standard Dev	0.019973616	0.018074696
Max	0.087626775	0.075098437
Min	0.002028398	0.000763632

As the reader can clearly see, the Morgan Method outperforms the Arnold Method slightly under these parameters. The average, standard deviation, max, and min are all lower, implying that the Morgan Method trends closer to zero, perhaps faster than the Arnold Method.

Difference. For the difference, we have simply taken each value for the Arnold Method, $|Arnold|_{(\beta, \alpha)}$, and subtracted from it $|Morgan|_{(\beta, \alpha)}$. This can tell us easily which of the values is closest to zero: if $|Arnold|_{(\beta, \alpha)} - |Morgan|_{(\beta, \alpha)}$ results in a negative value, then for that particular α and β Arnold is a better method, but if it is positive, then Morgan is better. Here are the results:

Negatives	Positives
-0.011001	0.042644
-0.023482	0.005632
-0.004105	0.024794
-0.011001	0.035748
-0.011001	0.023482
-0.038587	0.005632
-0.019425	0.005632
-0.011001	0.038587
-0.005632	0.016585
-0.002792	0.011001
-0.023482	0.053908
-0.004105	0.005632
-0.015058	0.016585
-0.045484	0.016585
-0.024794	0.033218
-0.001265	0.002792
-0.024794	0.045484
-0.011001	0.004105
-0.004105	0.016585
-0.009689	0.004105
-0.001265	0.026321
-0.004105	0.001265
-0.023482	0.024794
	0.017898
	0.016585

As the reader can see, if we take into consideration the difference between the two methods, then the Morgan Method is slightly superior to Arnold's, be it only by two values: it is closer to zero for 25 of the 48 tables, and Arnold's for 23.

The statistical and difference based approaches agree, if only narrowly, and we maintain that the Morgan Method is superior to Arnold's for a further reason, based on observations about the Galois Fields which are not exactly open to statistical criticism: the structure.

Under Arnold's Method, there are values which are more commonly repeated across the many tables of a Galois Field. For instance, here are four different tables selected from $p = 13$:

12	85	105	13	16	60	51	106	101	53	118	75	24	124
11	155	3	7	123	83	20	86	145	130	94	121	26	8
10	29	62	163	49	19	50	125	136	45	128	68	165	4
9	57	47	73	32	77	164	25	23	153	96	90	78	156
8	43	11	142	150	64	63	76	18	82	59	139	33	9
7	99	38	132	115	65	30	119	138	89	67	120	74	27
6	15	111	158	36	151	5	54	35	114	149	31	48	122
5	127	93	117	55	143	166	102	160	147	148	66	58	95
4	141	72	162	6	12	69	107	109	80	161	116	157	131
3	113	88	81	152	44	129	52	41	134	103	133	79	146
2	71	92	110	37	10	46	61	2	104	167	39	91	87
1	1	40	108	159	34	137	17	22	135	144	100	97	21
0	∞	168	70	112	140	126	14	98	42	56	28	154	84
	0	1	2	3	4	5	6	7	8	9	10	11	12

12	85	82	142	13	50	80	143	135	91	159	95	116	62
11	155	37	152	161	44	61	83	165	120	18	150	132	45
10	29	103	24	26	39	87	86	60	79	125	6	35	162
9	57	67	107	22	54	88	63	52	114	34	131	115	153
8	43	49	139	74	101	40	117	8	20	93	100	53	38
7	99	130	5	149	94	27	96	76	109	105	157	64	156
6	15	72	148	73	21	25	160	12	111	10	65	89	46
5	127	122	137	16	9	104	92	33	124	17	158	55	133
4	141	69	31	47	118	30	136	147	4	138	106	23	151
3	113	78	119	90	41	163	144	2	3	123	110	108	19
2	71	129	48	66	102	36	81	167	145	128	77	68	121
1	1	146	32	11	75	7	51	59	164	134	97	58	166
0	∞	168	70	112	140	126	14	98	42	56	28	154	84
	0	1	2	3	4	5	6	7	8	9	10	11	12

12	85	107	40	7	100	131	13	123	120	102	66	132	3
11	15	53	37	50	138	32	105	164	30	62	61	101	111
10	141	158	19	163	122	69	96	20	11	63	59	8	156
9	113	94	151	128	135	160	148	159	68	31	130	41	35
8	127	162	49	6	55	149	144	142	45	165	82	108	5
7	71	118	88	109	117	161	93	157	52	106	167	86	26
6	155	110	2	83	22	136	73	9	77	33	25	4	34
5	43	89	24	166	81	129	58	60	65	139	90	133	78
4	29	119	125	46	115	152	75	64	76	51	44	67	10
3	57	72	92	143	147	95	104	12	153	38	79	103	74
2	99	27	17	145	146	114	80	21	116	54	134	121	137
1	1	87	48	150	18	36	39	97	47	16	91	124	23
0	∞	168	98	56	28	42	154	70	126	112	140	14	84
	0	1	2	3	4	5	6	7	8	9	10	11	12

12	85	47	24	82	39	87	142	60	23	13	6	91	162
11	99	74	61	37	38	27	96	20	53	105	101	8	156
10	141	69	143	103	62	30	80	147	116	138	50	79	95
9	113	34	88	67	75	119	51	115	52	22	41	2	110
8	43	149	40	49	100	5	139	165	120	18	150	132	45
7	155	161	83	130	157	152	117	64	76	93	44	109	94
6	71	10	25	128	9	160	148	33	68	73	46	167	77
5	127	129	48	66	102	36	81	55	89	16	133	124	65
4	29	26	86	125	106	136	31	135	35	159	151	4	118
3	57	11	163	134	54	32	63	164	114	146	19	59	153
2	15	72	92	17	21	137	104	12	111	122	121	145	158
1	1	78	7	90	97	107	144	58	3	123	166	108	131
0	∞	168	14	56	28	126	70	154	42	112	140	98	84
	0	1	2	3	4	5	6	7	8	9	10	11	12

Figure 7: Four tables of $GF(13^2)$, for $A^2 = 2A + 7$, $A^2 = 3A + 7$, $A^2 = 6A + 2$ and $A^2 = 9A + 11$.

These tables were selected as “randomly” as we could manage, but you will notice that (though this be the case) the tables have a surprising number of similarities.

1. Along the first column and the bottom row of every table there tend to be values which are the same and which seem to not change, despite changes in many other places in the table. (Every value in the bottom row is a multiple of $p + 1 = 14$: the bottom row holds the nonzero integers mod p , and these are exactly the powers of A^{p+1} .)
2. Though we mentioned it at the start of this debate, the diagonals in the table have a surprising amount of predictability within each individual table, and you will recall from the beginning that every table has a “twin.”
3. Though this seems obvious to state, the ∞ in the bottom left corner is always there.

Given that these similarities exist, we assert that the Morgan Method does not count as many similarities both within individual Galois Tables and within the whole Galois Field as does the Arnold Method, thereby lending the Morgan Method the benefit of having more randomness than the former.

Still, over the course of our project, we were unable to provide a proof for either conjecture, implying that more work needs to be done to discover whether Vladimir Arnold is correct about the equidistribution of the Galois Fields. However, we were able to gather data about how predictable the many tables are within a given field.

The first trial of statistically analyzing the tables was: what do we measure? It was not as simple as taking the standard deviation or average about a table, as this would provide us with no knowledge whatsoever about the Galois Field. So, we began to collect data on individual squares within every single table iteration of a Galois Field.

We collected data from $p = 11, 13$ and 17 , but for purposes of brevity we are only presenting the data from $p = 17$, our largest table. Our most influential observation is this: that within individual cells, the values stick around the middle of the range of values. We argue that this implies something approaching equidistribution:

(u, v)	Mean	Median	(u, v)	Mean	Median	(u, v)	Mean	Median
(1, 1)	144.5	144.5	(3, 1)	150.5	151.0	(5, 1)	150.5	150.0
(1, 2)	150.5	144.0	(3, 2)	132.5	135.0	(5, 2)	126.5	125.0
(1, 3)	138.5	138.0	(3, 3)	144.5	144.5	(5, 3)	138.5	121.5
(1, 4)	144.5	139.0	(3, 4)	144.5	151.5	(5, 4)	144.5	145.0
(1, 5)	138.5	139.0	(3, 5)	150.5	167.5	(5, 5)	144.5	144.5
(1, 6)	144.5	130.5	(3, 6)	132.5	130.0	(5, 6)	132.5	130.5
(1, 7)	144.5	133.0	(3, 7)	150.5	150.5	(5, 7)	144.5	141.5
(1, 8)	168.5	193.5	(3, 8)	150.5	146.0	(5, 8)	150.5	153.0
(1, 9)	138.5	128.0	(3, 9)	138.5	122.0	(5, 9)	138.5	124.5
(1, 10)	144.5	128.0	(3, 10)	132.5	116.0	(5, 10)	138.5	133.5
(1, 11)	162.5	181.0	(3, 11)	150.5	152.5	(5, 11)	138.5	135.5
(1, 12)	150.5	155.5	(3, 12)	156.5	161.5	(5, 12)	138.5	133.0
(1, 13)	132.5	128.0	(3, 13)	132.5	130.5	(5, 13)	156.5	162.5
(1, 14)	144.5	141.5	(3, 14)	138.5	130.5	(5, 14)	156.5	161.0
(1, 15)	132.5	126.5	(3, 15)	138.5	137.5	(5, 15)	132.5	116.0
(1, 16)	132.5	128.0	(3, 16)	144.5	141.0	(5, 16)	156.5	155.0
(2, 1)	138.5	145.0	(4, 1)	144.5	150.0	(6, 1)	144.5	158.5
(2, 2)	144.5	144.5	(4, 2)	150.5	170.5	(6, 2)	156.5	165.5
(2, 3)	156.5	154.0	(4, 3)	144.5	137.5	(6, 3)	156.5	159.0
(2, 4)	138.5	118.5	(4, 4)	144.5	144.5	(6, 4)	156.5	159.5
(2, 5)	162.5	164.0	(4, 5)	144.5	144.0	(6, 5)	156.5	158.5
(2, 6)	132.5	123.5	(4, 6)	132.5	129.5	(6, 6)	144.5	144.5
(2, 7)	138.5	119.0	(4, 7)	138.5	137.0	(6, 7)	150.5	171.0
(2, 8)	150.5	158.0	(4, 8)	150.5	146.5	(6, 8)	150.5	163.5
(2, 9)	144.5	143.0	(4, 9)	144.5	139.5	(6, 9)	150.5	159.5
(2, 10)	150.5	151.5	(4, 10)	138.5	134.0	(6, 10)	144.5	156.5
(2, 11)	138.5	131.0	(4, 11)	150.5	161.5	(6, 11)	138.5	134.5
(2, 12)	144.5	141.5	(4, 12)	156.5	183.5	(6, 12)	132.5	129.5
(2, 13)	132.5	109.0	(4, 13)	132.5	120.5	(6, 13)	162.5	174.0
(2, 14)	132.5	118.5	(4, 14)	138.5	136.5	(6, 14)	144.5	151.5
(2, 15)	138.5	137.5	(4, 15)	132.5	121.5	(6, 15)	138.5	125.0
(2, 16)	120.5	110.0	(4, 16)	120.5	102.5	(6, 16)	156.5	180.5

This table seems complicated, and has many rows, but it is not exactly obvious what a given entry of mean and median represents. Consider a value for (u, v) , say $(6, 9)$, with a mean of 150.5 and a median of 159.5. This means that across every single one of the 48 tables in $p = 17$, the value in column 6 and row 9 has mean 150.5 and median 159.5. The same could be extended to all cells of the table.

After a very brief examination of the table above, you will no doubt find that the values center around $\frac{1}{2}p^2 = 144.5$, the average of all the values $1, 2, \dots, p^2 - 1$ in a table: the means of the 96 cells lie between 120.5

and 168.5, and the medians, more widely spread, between 102.5 and 193.5. In general, a study in the future might try to verify whether this extends to prime values greater than 17.

We assert that this implies a roughly equal or equitable distribution of values within every single table. For if the values within the tables deviate or are weighted too heavily above $\frac{1}{2}p^2$ or below it, then there would be a disparate number of coordinates whose means and medians are quite far away from the midpoint.

This, we believe, is our most valid evidence that the Galois Fields are equidistributed, despite our misgivings about the rudimentary and theoretical mess created by applying measurements like mean and median to something as complex as a finite field.

FUTURE WORK

Over the course of eight weeks of study much has been learned, and what has been gained is hopefully established above, but what we must also point out is where we have failed, where we have come short (as these are no doubt the most important) and which mathematicians should continue to study in the future. These are the gaps that we have not been able to fill.

The foremost matters arise in our failure to produce a sufficient proof for Vladimir Arnold's Conjecture; this said, we did not expect to provide one during our study, given that it would require far longer inquiry. But nor were we truly capable of specifying that it might exist, or that it at least appears to exist. Indeed, the best we can do is a "wholesome maybe." In our search for statistical randomness we have admittedly come up with crumbs.

One of the initial problems in our study was the code implemented. Though we automated the process of obtaining individual tables within a Galois Field to a far more efficient state than can be done by hand, we were severely limited by our ability to fill tables with the data generated by our code. We started off with the most rudimentary code, that which could generate a single table, followed by more complex iterations till we eventually wrote code which could find every single "viable" table within a Galois Field. This drastically changed our scope of study, since it enabled us to generate tables as large as $p = 17$, which has 48 associated tables, but took roughly five or ten minutes to compute, and then almost two or three hours to convert by clicking and pasting into an Excel file to turn them into the tables the reader has seen above. It was an incredibly painstaking process, and our abilities at writing code were not sufficient to move onto the next prime value.¹

What is needed most to further the study is a computer based approach: a code written which not only generates the fields for a prime number, but which also fills and outputs the resulting tables and provides strings of coordinate data associated with each value in the table.

And most importantly, the study of Galois Fields is not nearly complete. We know much about them, about their structure and behavior; we even have whole theorems that pertain to Galois Fields (by way of applying to finite fields). However, juxtaposed with the unknown, our knowledge is the tip of the iceberg.

There are other areas outlined in Vladimir Arnold's book which we were not able to go into, but which directly relate to the study. For instance, there is a whole subclass called Distribution of Geometric Progressions of Residues, which evaded our study, and another about Projective Structures which has been equally elusive (Arnold, 2011, pp. 37 & 44). From the depths of the structure to the infinite intricacies, what is needed deeply are those willing to study these structures to provide a continuance of Arnold's work.

¹The tables, figures and measurements in this version of the paper have been redrawn and recomputed by Python code written since the original study. Every table of the first thousand primes can now be drawn, with its twin and both measures, at <https://maths.dsmorgan.com/papers/harmony-amid-chaos/explore>.

CONCLUSION

The Galois Fields were a daunting task at the start, requiring much mathematical explanation and understanding before we were even able to delve deeply into their harmony and chaos. This said, we were capable of showing several things for ourselves. On Harmony, we have concluded that the structure within a Galois Field is filled with enough order that proofs can be made between tables, but it is also chock full of uncertainties, of Chaos.

The Harmony of a Galois Field is easily defined by the three proofs we have shown:

1. If $A_i^2 = \alpha A_i + \beta$ has no integer solutions mod p , then $A_k^2 = -\alpha A_k + \beta$ has no integer solutions mod p .
2. If $A_1^n = \alpha' A_1 + \beta'$, $A_1^2 = \alpha A_1 + \beta$ and $A_2^2 = -\alpha A_2 + \beta$, then there is a table where $A_2^n = -\alpha' A_2 + \beta'$ if n is even and $A_2^n = \alpha' A_2 - \beta'$ if n is odd.
3. Suppose that $A_1^2 = \alpha A_1 + \beta$ and $A_2^2 = -\alpha A_2 + \beta$; then if the powers on A_1 generate the Galois Field with p^2 elements, $\{A_1, A_1^2, A_1^3, \dots, A_1^{p^2-1}\}$ where $A_1^{p^2-1} = 1$, then the powers on A_2 also generate the Galois Field with p^2 elements.

But as for Chaos, that which cannot be proven, we have no proofs to bear. We are empty handed. However, we did collect data.

Data is by far the most important aspect of our study. There was almost nothing out there on Galois Fields that a first-year math student could really understand. There are plenty of complex books on finite fields, but none that are very attainable for a first-year math student. Arnold's book provided an intuitive way of expressing these fields. What was needed is exploration, and that is what we have provided. Our inquiry has observed the following:

1. Vladimir Arnold's Method, and Morgan's slight improvement, show promise at being proved one day, since they at least appear to grow closer to zero as p grows.
2. The fields appear to have the hallmark of randomness, defined by a propensity to be uniformly distributed on a per-cell basis, and this property might lend credence to equidistribution if it cannot be shown by either method above.

It may seem like nothing, given our eight weeks of study, but it is a start. Can it not be hypothesized that we might know more about Galois Fields if they were observed with the same intensity as the prime numbers? People have been hunting for the next largest prime number since the dawn of the byte. If they had had similar vigor for Galois Fields, perhaps we would not be writing this paper. While we have little to show, it is our hope that our study is the first of many that will be conducted one day.

It is to those who would conduct them, to those who would answer the call, that our paper is written. We hope that it provides at least moderate, if not ample, inquiry into Galois Fields and that someone might one day make harmony out of this chaotic branch of Mathematics.

REFERENCES

- Arnold, V. I. (2011). *Dynamics, statistics and projective geometry of Galois fields*. Cambridge: Cambridge University Press.
- Lidl, R., & Niederreiter, H. (1997). *Finite fields* (2nd ed.). Cambridge: Cambridge University Press.