Olivet Nazarene University
Digital Commons @ Olivet

Pence-Boyce STEM Student Scholarship

Summer 2020

# Harmony Amid Chaos

Drew Schaffner
*Olivet Nazarene University*, dmschaffner@olivet.edu

Follow this and additional works at: https://digitalcommons.olivet.edu/pence_boyce

 Part of the Algebra Commons, Algebraic Geometry Commons, Geometry and Topology Commons, Number Theory Commons, Other Mathematics Commons, Other Statistics and Probability Commons, Set Theory Commons, and the Statistical Theory Commons

## Recommended Citation

Schaffner, Drew, "Harmony Amid Chaos" (2020). *Pence-Boyce STEM Student Scholarship*. 13.
https://digitalcommons.olivet.edu/pence_boyce/13

This Thesis is brought to you for free and open access by Digital Commons @ Olivet. It has been accepted for inclusion in Pence-Boyce STEM Student Scholarship by an authorized administrator of Digital Commons @ Olivet. For more information, please contact digitalcommons@olivet.edu.

# HARMONY AMID CHAOS

Measuring the Randomness of Galois Fields

By 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 bounded under the operations of multiplication and addition, (with associative, commutative, and distributive properties) such that every nonzero element has both an additive inverse and a multiplicative inverse.

Consider a prime number, $p$, a field can be formed by the residues of modulo $p$. For instance, the simplest field, $p = 2$:

I should like to introduce the notation, $GF(p)$, taking $p = 2$, to mean the group:

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

A simple check ensures that operations in this group are closed under inverses in multiplication and addition (note that since we are adding and multiplying by elements in $Z/2Z$ that the operation set will be closed):

$$0 + 0 = 0, \quad 0 + 1 = 1, \quad 1 + 1 = 0,$$
$$0 \cdot 0 = 0, \quad 0 \cdot 1 = 0, \quad 1 \cdot 0 = 0, \quad 1 \cdot 1 = 1.$$

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 $Z/4Z = \{0, 1, 2, 3\}$ 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 1800's by a young mathematician named Evariste Galois, they are part of a subset of fields that are finite and are given the name

Galois Fields to honor their creator, who produced two theorems relating to finite fields that 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. *The field of $p^n$ elements is defined explicitly with the number of elements it contains up to isomorphism.*

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:

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

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 $\alpha$ and $\beta$ 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:

$$0+0=0,\ \ 0+1=1,\ \ 0+A=A,\ \ 0+A+1=A+1,$$

$$1+1=0,\ \ 1+A=1+A,\ \ 1+A+1=A,$$

$$A+A=0,\ \ A+A+1=1,$$

$$A+1+A+1=0.$$

$$0*0=0,\ \ 0*1=0,\ \ 0*A=0,\ \ 0*(A+1)=0,$$

$$1 * 1 = 1,\ \ 1 * A = A,\ \ 1 * (A + 1) = A + 1,$$

$$A * A = A^2,\ \ A * (A + 1) = A^2 + A,$$

$$(A + 1) * (A + 1) = A^2 + 1.$$

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 $A^2,\ A^2 + A,\ A^2 + 1$ 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 affect saying, "The square root of negative one does not exist, therefore, let us create this strange value, "$i$" such that the $\sqrt{-1} = i$." 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?

$$A * A = A^2 = A + 1,\ \ A * (A + 1) = A^2 + A = A + 1 + A = 1,$$

$$(A + 1) * (A + 1) = A^2 + 1 = A + 1 + 1 = A.$$

The problem is alleviated; as we can see, the field is still closed, none of the elements are outside the initial set, and every nonzero element still has an additive and 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, $A + 1$ would have two multiplicative inverses. 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 $A$:

$$A^2 = A + 1,$$

$$A^3 = A^2 + A = A + 1 + 1 = 1,$$

$$A^4 = A.$$

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 $\alpha$ and $\beta$ are "good" choices: then we can express the values of $A^k$, where $k \leq p^2 - 1$, as the expression:

$$A^k = v_k * A + u_k * 1,$$

$$where \;\; v_{k+1} = \alpha v_k + u_k \;\; and \;\; u_{k+1} = \beta v_k.$$

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:

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

Consider the table expressing the powers on $A^k$ akin to a table of logarithms, whereby the elements inside the tables represent the power on $A$ and the index represent the values $(u_k, k_k)$:

| | | |
|---|---|---|
| 1 | 1 | 2 |
| 0 | ∞ | 3 |
| | 0 | 1 |

The use of the infinity symbol is based on the $\log(0) = -\infty$, we denote this value as positive ∞, since we do not know whether A is positive or 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 field (choices for $\alpha$ and $\beta$) 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 $\alpha$ and $\beta$ 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 $\alpha$ and $\beta$. 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 elements in a field, to fix the number of unique elements generated by the field, and generate the whole field, if the recursive formula and the choice of $\alpha$ and $\beta$ generates unique values for the first $p^2$ (in this case 49) elements then we keep the table (include it as one of the 8). If, however, the recursive formula and the choice for $\alpha$ and $\beta$ repeats

before cycling through all 49 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 before hand, simply iterates the recursive formula 49 times with a particular $\alpha$ and $\beta$, and tells whether it should be included or excluded based on the uniqueness of the elements produced in the string with length 49. 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 factors. That is, if you were to try and solve the equation using the quadratic formula you would get non integer solutions, then that choice for $\alpha$ and $\beta$ is likely to generate the set of elements in the Galois Field.

Notice our use of the phrase "likely." 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 $\alpha$ and $\beta$ 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 factors, but you can draw out all the possible combinations for $\alpha$ and $\beta$ and you will find that there are 3 other choices for $A^2$ that do not have integer factors. But this is a great improvement given our knowledge of how many possible combinations there are for $\alpha$ and $\beta$. In $p = 5$ there are 25 combinations, excluding those with integer solutions, there are 7, only 4 of which end up generating the whole set (those being the ones above).

In sum, we can rid ourselves of the brute force method of iterating every single combination for $\alpha$ and $\beta$ 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 across the diagonal. 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 $p = 17$ 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 | i | 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 |

| | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 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 | i | 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 |

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 the table above, 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 $p$:

In general, the bottom right corner of the Galois Table is always $\frac{1}{2}(p^2 - 1)$, if we suppose that $x = \frac{1}{2}(p^2 - 1)$, and that $A^x = -1$ or $p - 1$. And thereby if we suppose there is some value $a \in Z/pZ$ where $A^a$ is defined by the table. Multiplying $A^x$ by $A^a$ yields $-A^a$ and it is precisely this that produces the symmetry defined above.

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 arms of the diagonal rotate about one another when looking between the two tables. The odd values that flip across a vertical line through the center of the diagonal,

and the even values flip across a similar horizontal line. 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 | i | 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 | i | 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 |

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.

### Theorem 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.*

Proof:

Let $A_i^2 = \alpha * A_i + \beta$. We take this to mean that $GF(p^2)$, $A_i^2$ has no integer factors for $\alpha$ and $\beta$. Such a solution 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 $A_k^2$ equal to zero, such that:

$$A_k^2 + \alpha * A_k - \beta = 0,$$

Where, $-\beta = c_1 * c_2$ and $\alpha = c_1 + c_2$ s.t. $c_1, c_2 \in Z/pZ$, therefore,

$$(A_k + c_1) * (A_k + c_2) = 0.$$

Suppose that we were to set $A_i^2$ equal to zero and attempt to find integer solutions based on the factors of $A_k^2$.

$$A_i^2 - \alpha * A_i - \beta = 0,$$

We can take the negative of the solution for $\alpha$ in the previous equation, and $\beta$ will remain the same,

$$-\alpha = c_1 + c_2, \qquad -\beta = c_1 * c_2,$$

We obtain that $A_i^2$ has integer solutions, a contradiction, since $A_i^2$ does not have integer solutions.

Therefore, by contradiction, if $A_i^2 = \alpha * A_i + \beta$, then there is a table where $A_k^2 = -\alpha * A_k + \beta$.

Q.E.D.

**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 also let $A_1^2 = \alpha A_1 + \beta$ and $A_2^2 = -\alpha A_2 + \beta$.

First case, n is even:

For induction, $k$ is even, $k-1$ is odd.

$$A_1^{k-1} = \alpha' A_1 + \beta' \qquad A_2^{k-1} = \alpha' A_2 - \beta'$$
$$A_1^{k-1} A_1 = \alpha' A_1^2 + \beta' A_1 \qquad A_2^{k-1} A_2 = \alpha' A_2^2 - \beta' A_2$$
$$A_1^k = a'(\alpha A_1 + \beta) + \beta' A_1 \qquad A_2^k = a'(-\alpha A_2 + \beta) - \beta' A_2$$
$$A_1^k = (\alpha'\alpha + \beta') A_1 + a'\beta \qquad A_2^k = -(\alpha'\alpha + \beta') A_2 + a'\beta$$

Second case, n is odd:

For induction, $k$ is odd, $k-1$ is even.

$$A_1^{k-1} = \alpha' A_1 + \beta' \qquad A_2^{k-1} = -\alpha' A_2 + \beta'$$

$$A_1^{k-1}A_1 = \alpha' A_1^2 + \beta' A_1 \qquad A_2^{k-1}A_2 = -\alpha' A_2^2 + \beta' A_2$$
$$A_1^k = a'(\alpha A_1 + \beta) + \beta' A_1 \qquad A_2^k = -a'(-\alpha A_2 + \beta) + \beta' A_2$$
$$A_1^k = (\alpha'\alpha + \beta')A_1 + a'\beta \qquad A_2^k = (\alpha'\alpha + \beta')A_2 - a'\beta$$

Therefore, by the laws of induction, it follows: If $A_1^n = \alpha' A_1 + \beta'$, 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.

Q.E.D.

**Theorem 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* $\{A_1, A_2, A_3, \dots, A_1^{p^2-1}\}$ *where* $A_1^{p^2-1} = 1$*, then the powers on* $A_2$ *also generate the Galois Field with* $p^2$ *elements.*

Proof:

Let $A_1^2 = \alpha * A_1 + \beta$ and $A_2^2 = -\alpha * A_2 + \beta$ and let $A_1^{p^2-1} = 1$

Suppose for contradiction that $A_2^i = 1$ for $i < p^2 - 1$, meaning that the succeeding powers on $A_2^i$ repeat elements before wrapping all the way through the nonzero elements of $GF(p^2)$.

And allow **Theorem 2** to be introduced to differentiate the powers on $A_2$ into two cases:

Odd Case:

Suppose $i$ is odd. By Theorem 2, $A_1^i = \alpha' A_1 + \beta'$ and $A_2^i = \alpha' A_2 - \beta'$. Therefore since $A_2^i = 1$ we have $\alpha' = 0$ and $\beta' = p - 1$, and thus $A_1^i = p - 1$. Squaring $A_1^i$ yields:

$$A_1^{2i} = (p-1)^2 = 1 \; mod \; p,$$

recall that,

$$A_1^{p^2-1} = 1,$$

This implies that $2i = p^2 - 1$ as statement which is true, since $p^2 - 1 = (p-1)(p+1)$ a number that is always divisible by 4 since $p - 1$ and $p + 1$ are both even integers. But this a contradiction, since it implies that $i$ is divisible for 2.

Even Case:

Suppose that $i$ is even. By Theorem 2, $A_1^i = \alpha' A_1 + \beta'$ and $A_2^i = -\alpha' A_2 + \beta'$. And recall $A_2^i = 1$ implying that $\alpha' = 0$ and $\beta' = 1$. This is a contradiction since it implies that $i = p^2 - 1$ and if the reader will recall, we constrained $i < p^2 - 1$.

Therefore, by cases, if the powers on $A_1$ generate the Galois Field with $p^2$elements $\{A_1^1, A_1^2, A_1^3, \dots, A_1^{p^2-1}\}$ where $A_1^{p^2-1} = 1$, then the powers on $A_2$ also generate the Galois Field with $p^2$elements.

Q.E.D.

## 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 discernable structure evident that there is some sort of underlying structure which we are unable to identify, or evident 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 a proportion of elements in the section. Then we shall take N to mean the number of occurrences of values in the Galois Field, less than a value $m$, which occur in the region $G$. Then the fraction of $N/m$, is the proportion of $N$ to the value of $m$ (Arnold, 2011, p. 17).

Arnold proposes: "The $\lim_{p\to\infty} \frac{N}{m} = \frac{G}{z}$" (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 $\alpha$ and $\beta$. 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 choice of $\alpha$ and $\beta$ and the resulting $|Arnold|$ is taken by subtracting one side of the equation from the other and then taking the absolute value.

| $(\beta, \alpha)$ | $\lvert Arnold \rvert$ | $(\beta, \alpha)$ | $\lvert Arnold \rvert$ |
|---|---|---|---|
| (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) | 0.05030426 |
| (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 one of the diagonals into consideration, but it does, as I have outlined a hypothetical area $N$ 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 | i | 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 |

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 of $G/z$ to the proportion of $N/m$, 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 | 164 | 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 | 133 | 94 | 23 | 47 | 130 |
| 8 | 127 | 62 | 32 | 53 | 117 | 45 | 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 | i | 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 |

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. 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 $p$.

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.

| $(\beta, \alpha)$ | $\lvert Morgan \rvert$ | $(\beta, \alpha)$ | $\lvert Morgan \rvert$ |
|---|---|---|---|
| (3, 4) | 0.014556735 | (10, 1) | 0.013029471 |
| (3, 6) | 0.00613292 | (10, 4) | 0.000763632 |
| (3, 7) | 0.007660184 | (10, 5) | 0.013029471 |
| (3, 10) | 0.007660184 | (10, 12) | 0.00613292 |
| (3, 11) | 0.00613292 | (10, 13) | 0.013029471 |
| (3, 13) | 0.033719127 | (10, 16) | 0.007660184 |

| | | | |
|---|---|---|---|
| (5, 2) | 0.026822575 | (11, 2) | 0.055936046 |
| (5, 3) | 0.021453287 | (11, 6) | 0.019926023 |
| (5, 5) | 0.019926023 | (11, 8) | 0.035246391 |
| (5, 12) | 0.026822575 | (11, 9) | 0.054408782 |
| (5, 14) | 0.00613292 | (11, 11) | 0.068201885 |
| (5, 15) | 0.026822575 | (11, 15) | 0.019926023 |
| (6, 2) | 0.04751223 | (12, 3) | 0.026822575 |
| (6, 7) | 0.040615678 | (12, 5) | 0.040615678 |
| (6, 8) | 0.068201885 | (12, 8) | 0.013029471 |
| (6, 9) | 0.014556735 | (12, 9) | 0.000763632 |
| (6, 10) | 0.033719127 | (12, 12) | 0.014556735 |
| (6, 15) | 0.00613292 | (12, 14) | 0.014556735 |
| (7, 1) | 0.007660184 | (14, 1) | 0.00613292 |
| (7, 3) | 0.014556735 | (14, 6) | 0.062832598 |
| (7, 4) | 0.035246391 | (14, 7) | 0.035246391 |
| (7, 13) | 0.00613292 | (14, 10) | 0.019926023 |
| (7, 14) | 0.00613292 | (14, 11) | 0.028349839 |
| (7, 16) | 0.00613292 | (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 $\alpha$ and $\beta$:

**Statistical:**

| | Arnold | Morgan |
|---|---|---|
| Average | 0.025946586 | .022941276 |
| Standard Dev | 0.019973616 | .01786713 |
| Max | 0.087626775 | .068201885 |
| Min | 0.002028398 | .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 and Morgan Method, and taken $Arnold_{(\beta,\alpha)}$ 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 $\alpha$ and $\beta$ Arnold is a better method, but if it is positive, then Morgan is better. Here are the results:

| Negatives | Positives |
|---|---|
| -0.0041 | 0.042644 |
| -0.00816 | 0.019425 |
| -0.00969 | 0.024794 |
| -0.0179 | 0.028851 |
| -0.00126 | 0.023482 |
| -0.0179 | 0.033218 |
| -0.0179 | 0.016585 |
| -0.05238 | 0.005632 |
| -0.01253 | 0.053908 |
| -0.0179 | 0.002792 |
| -0.00563 | 0.005632 |
| -0.00969 | 0.021954 |
| -0.03038 | 0.016585 |
| 0.033218 | 0.004105 |
| 0.038587 | 0.016585 |
| -0.00816 | 0.004105 |
| -0.0041 | 0.031691 |
| -0.03859 | 0.001265 |
| -0.0179 | 0.005632 |

| | |
|---|---|
| -0.00126 | 0.024794 |
| -0.02479 | 0.024794 |
| -0.0179 | 0.002792 |
| -0.0041 | 0.016585 |
| -0.00969 | |
| -0.02348 | |

As the reader can see, if we take into consideration the difference between the two methods, then Arnold's Method is slightly superior to ours (be it only by two values).

The statistical and difference based approaches have yielded different results, but we maintain that the Morgan Method is superior to Arnold's 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 | i | 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 | i | 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 | i | 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 | i | 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 |

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 last rows 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.
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 redefinition to "i" 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 both $p = 11, 13$ 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 across the Morgan range of values (the upper triangle), the values stick around $p^2 - 1$. We argue that this implies something approaching equidistribution:

| $(\beta, \alpha)$ | Mean | Median | $(\beta, \alpha)$ | Mean | Median | $(\beta, \alpha)$ | Mean | Median |
|---|---|---|---|---|---|---|---|---|
| (1, 1) | 145 | 145 | (3, 1) | 151 | 151 | (5, 1) | 151 | 150 |
| (1, 10) | 145 | 128 | (3, 10) | 133 | 116 | (5, 10) | 139 | 134 |
| (1, 11) | 163 | 181 | (3, 11) | 151 | 153 | (5, 11) | 139 | 136 |
| (1, 12) | 151 | 156 | (3, 12) | 157 | 162 | (5, 12) | 139 | 133 |
| (1, 13) | 133 | 128 | (3, 13) | 133 | 131 | (5, 13) | 157 | 163 |
| (1, 14) | 145 | 142 | (3, 14) | 139 | 131 | (5, 14) | 157 | 161 |
| (1, 15) | 133 | 127 | (3, 15) | 139 | 138 | (5, 15) | 133 | 116 |
| (1, 16) | 133 | 128 | (3, 16) | 145 | 141 | (5, 16) | 157 | 155 |
| (1, 2) | 151 | 144 | (3, 2) | 133 | 135 | (5, 2) | 127 | 125 |
| (1, 3) | 139 | 138 | (3, 3) | 145 | 145 | (5, 3) | 139 | 122 |
| (1, 4) | 145 | 139 | (3, 4) | 145 | 152 | (5, 4) | 145 | 145 |
| (1, 5) | 139 | 139 | (3, 5) | 151 | 168 | (5, 5) | 145 | 145 |
| (1, 6) | 145 | 131 | (3, 6) | 133 | 130 | (5, 6) | 133 | 131 |
| (1, 7) | 145 | 133 | (3, 7) | 151 | 151 | (5, 7) | 145 | 142 |
| (1, 8) | 169 | 194 | (3, 8) | 151 | 146 | (5, 8) | 151 | 153 |
| (1, 9) | 139 | 128 | (3, 9) | 139 | 122 | (5, 9) | 139 | 125 |
| (2, 1) | 139 | 145 | (4, 1) | 145 | 150 | (6, 1) | 145 | 159 |
| (2, 10) | 151 | 152 | (4, 10) | 139 | 134 | (6, 10) | 145 | 157 |
| (2, 11) | 139 | 131 | (4, 11) | 151 | 162 | (6, 11) | 139 | 135 |
| (2, 12) | 145 | 142 | (4, 12) | 157 | 184 | (6, 12) | 133 | 130 |
| (2, 13) | 133 | 109 | (4, 13) | 133 | 121 | (6, 13) | 163 | 174 |
| (2, 14) | Mean | Median | (4, 14) | Mean | Median | (6, 14) | Mean | Median |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| (2, 15) | 133 | 119 | (4, 15) | 139 | 137 | (6, 15) | 145 | 152 |
| (2, 16) | 139 | 138 | (4, 16) | 133 | 122 | (6, 16) | 139 | 125 |
| (2, 2) | 121 | 110 | (4, 2) | 121 | 103 | (6, 2) | 157 | 181 |
| (2, 3) | 145 | 145 | (4, 3) | 151 | 171 | (6, 3) | 157 | 166 |
| (2, 4) | 157 | 154 | (4, 4) | 145 | 138 | (6, 4) | 157 | 159 |
| (2, 5) | 139 | 119 | (4, 5) | 145 | 145 | (6, 5) | 157 | 160 |
| (2, 6) | 163 | 164 | (4, 6) | 145 | 144 | (6, 6) | 157 | 159 |
| (2, 7) | 133 | 124 | (4, 7) | 133 | 130 | (6, 7) | 145 | 145 |
| (2, 8) | 139 | 119 | (4, 8) | 139 | 137 | (6, 8) | 151 | 171 |
| (2, 9) | 151 | 158 | (4, 9) | 151 | 147 | (6, 9) | 151 | 164 |

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 $(\beta, \alpha)$, say the last entry in the bottom right corner, for $(6,9)$ with a mean of $151$ and median of $164$. This implies that for every single table in $p = 17$, the mean value for all entries in this column and row is $151$ and the median is $164$. The same could be extended to all values of the table.

After a very brief examination of the table above, you will no doubt find that all of the values center around $\frac{p^2-1}{2}$ for both the mean and median, no matter the coordinate, in general, a study in the future might try to verify whether this is extended 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 $\frac{p^2-1}{2}$ or below it, then there would be a disparate number of coordinates whose Mean's and Median's 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 8 weeks of study much has been learned, and what has been gained is hopefully established above, but what we must do now is state the areas in which 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 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.

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, p. 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.

## 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 which have not been shown before: 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 also chock full of uncertainties, of Chaos.

The Harmony of a Galois Field is easily defined by 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* $\{A_1, A_2 A_i, A_3, \dots, A_1^{p^2-1}\}$ *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 bare. 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 that 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 more than has been discovered in the near two hundred years since Evariste Galois first began to theorize these Mathematical objects. 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, we bring more than has been brought in the past. It is our study which is the first of studies that will hopefully 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.