PATTERNS IN ORDERS OF ELLIPTIC CURVES OVER FINITE FIELDS

3 messages

George Lambert <marchon@gmail.com> Tue, Jul 7, 2015 at 7:46 AM
To: bradfordtuckfield@gmail.com, bradford@analytics-man.com, George Lambert <marchon@gmail.com>
Cc: Darren Tapp <dtapp@email.hesser.edu>, dtappmath@facebook.com

Dear Bradford Tuckfield;

Summary: I am wondering if you could give me a little bit more information about exactly how the tables that were created in this paper were constructed, and was hoping you might have and would share the code used to brute force the primes up to 600 referred to in the paper.

Longer Explanation:

Last night I stumbled up this paper that you co-authored, Patterns in Orders of Elliptic Curves over Finite Fields.

To be honest, I am a Computer Software Architect not an a professionally trained mathematician. But I have spent over 2,000 hours reading, watching videos and trying to teach myself enough to understand how and why Elliptic Curves over Finite Fields work and their application in digital signatures and cryptography. But with that said - I am still trying to put the pieces together like a jigsaw puzzle.

As I was re-reading your paper for the second time to try to absorb all of the detail, I began pondering and exploring additional patterns in the tables that were in the paper.

Before long I noticed a few things that were interesting, but I could not immediately identify what. In the F11 Table - I noticed a numerical grouping that vaguely reminded me of a "Pascal's Triangle Arrangement" but there were numbers that just did not make sense. When I converted the numbers mod 11, interesting pictures began to emerge.

I organized all of the values into colors and filled in the grid (I have attached it - for you to see.) This took me down the road of trying to understand it, even more. I looked at the convergence of elements into the center of the grid, and found that there are 4 quadrants that appear to be mirrored. Even more interestingly - if one dissects one of the quadrants you find a line that stretches diagonally and is mirrored in the opposing diagonal quadrant. On each side of the diagonal the elements are mirrored as well displaying an interesting symmetry.

To try to more easily identify patterns I replaced the numbers mod 11 with arbitrary symbols to make recognition easier, and saw my speculation come into fascinating illustration (at least to the untrained mind that did not write your paper).

While doing your research did you notice these patterns and symmetries?

I would like to investigate more, but I wanted to make sure that I was producing and processing the data correctly. I have done additional experimentation on the F13 table, and detected a pattern for the frequency of the groups of common lines.

The Groups in F13 - {0}, {1,3,9}, {2,5,6}, {7,8,9}, {4,10,12}

Which I called:

A: {1,3,9}
B: {2,5,6}
C: {7,8,9}
D: {4,10,12}

I discovered that if I divided the grid at the center 6,6

There was a symmetric reflection pattern in the order of the lines.

Note that the progression of the lines from the center horizontally fits a pattern:

A's Reflect D's
B's Reflect C's

```
A B A D B B || C C A D C D
   ^ ||  |  \  /       \  /  |   || ^
   ^ ||  ------------------  || ^
   ^ ============== ^
   ^^^^^^^^^^^^^^^^^^^^
```

The 0 line - the outlier brought another pattern to my attention which was the reflection of values from the center line, which I believed might be repeated on the other lines, before I decided that this investigation was better done in python so that it could be replicated and run over the test cases described in your paper.

So back to my original question, could I get a small amount of assistance in making sure that I can construct the tables correctly.

Thank You

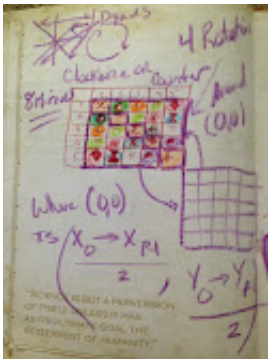
George Lambert.

@marchon
marchon@gmail.com
603-315-2105

6 attachments

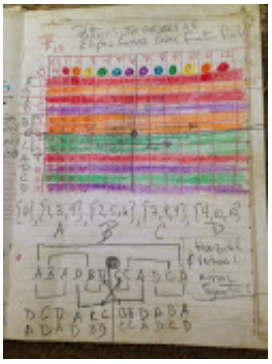
BinomialTriangle.gif
16K

IMG_2420.JPG
490K



IMG_2422.JPG
430K

IMG_2423.JPG
499K



IMG_2424.JPG
454K

PatternsInFiniteFields.pdf
262K