



Elliptic fields

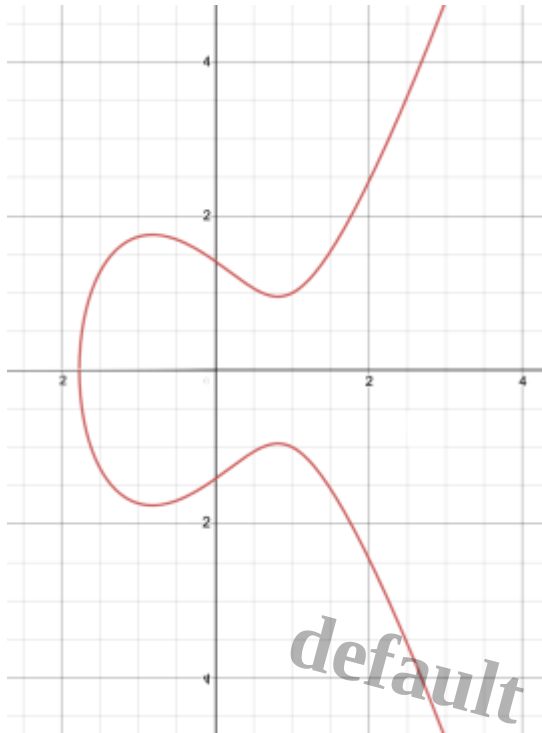
Description

One property of algebraic equations is that you can perform the same simple arithmetical operation on both sides of the equation and the equivalence still holds for the same x and y values, e.g. $y = 2x$ has the same values if both sides are multiplied by the same number e.g. $6y = 12x$. The same applies if either side of the equation is raised to the same power: $y^2 = (2x)^2$.

However, that kind of equivalence doesn't apply in the case of the **mod** operation, i.e. dividing both sides of the equation by the same divisor and just leaving the remainder. $y \bmod 3 = 2x \bmod 3$ is true for a different set of values for x and y than $y = 2x$. The graph of the relationship between x and y in the case of the mod variant will be different than for $y = 2x$, as I will show below for the elliptic curve.

Elliptic curve cryptography starts with more complex equations than $y = 2x$. As I explored in the post [Elliptic trapdoors](#), elliptic curves follow a general formula $y^2 = x^3 + ax + b$. (Such elliptic curves carry certain advantages, notably that you can perform repeated addition and scalar multiplication on values along the curve such that it's very difficult to reverse the process to discover the starting values.) Here's the curve for

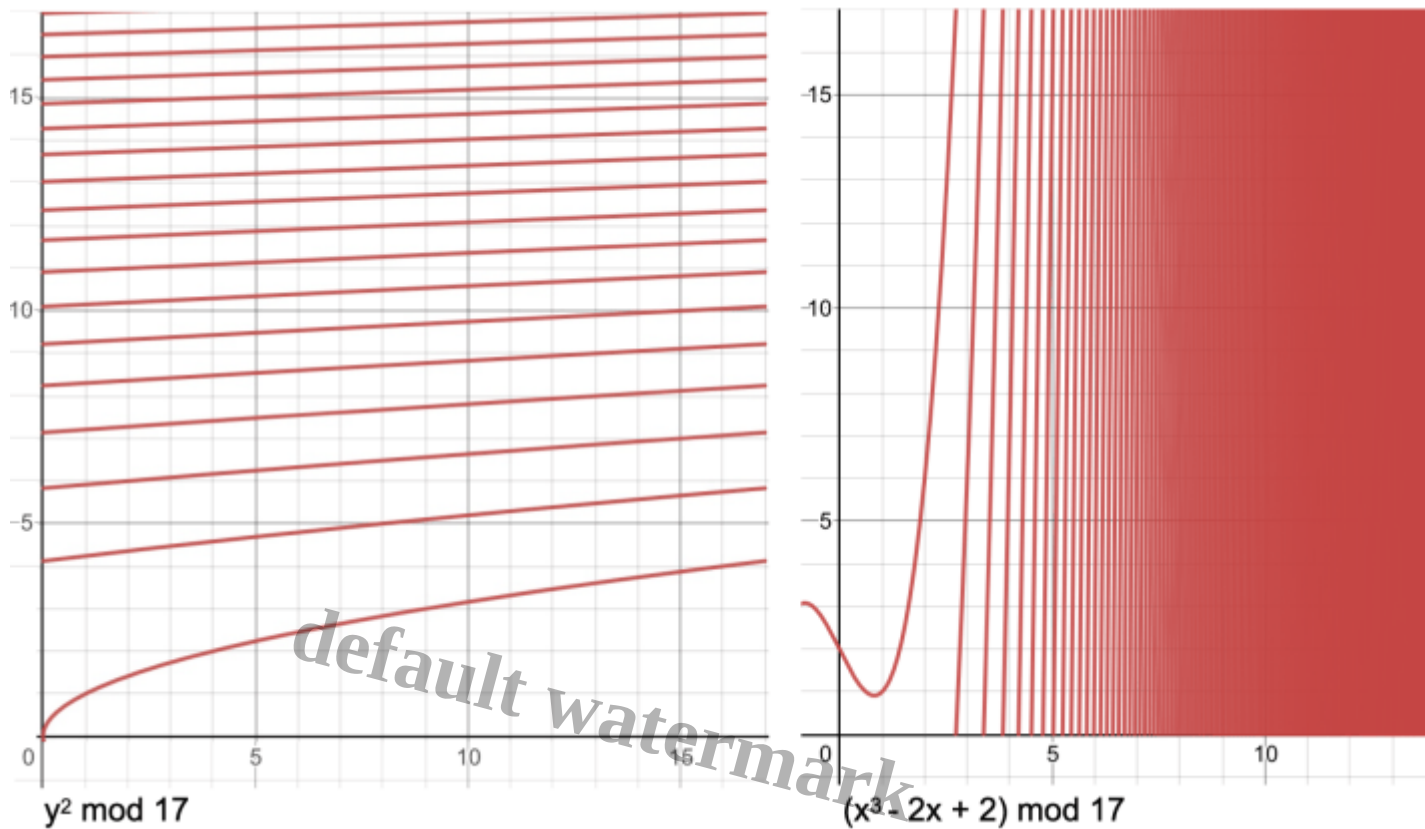
$$y^2 = x^3 + 2x + 2.$$



You can mod both sides of the elliptic curve equation by the same divisor. Iâ??ve chosen 17 as the divisor arbitrarily.

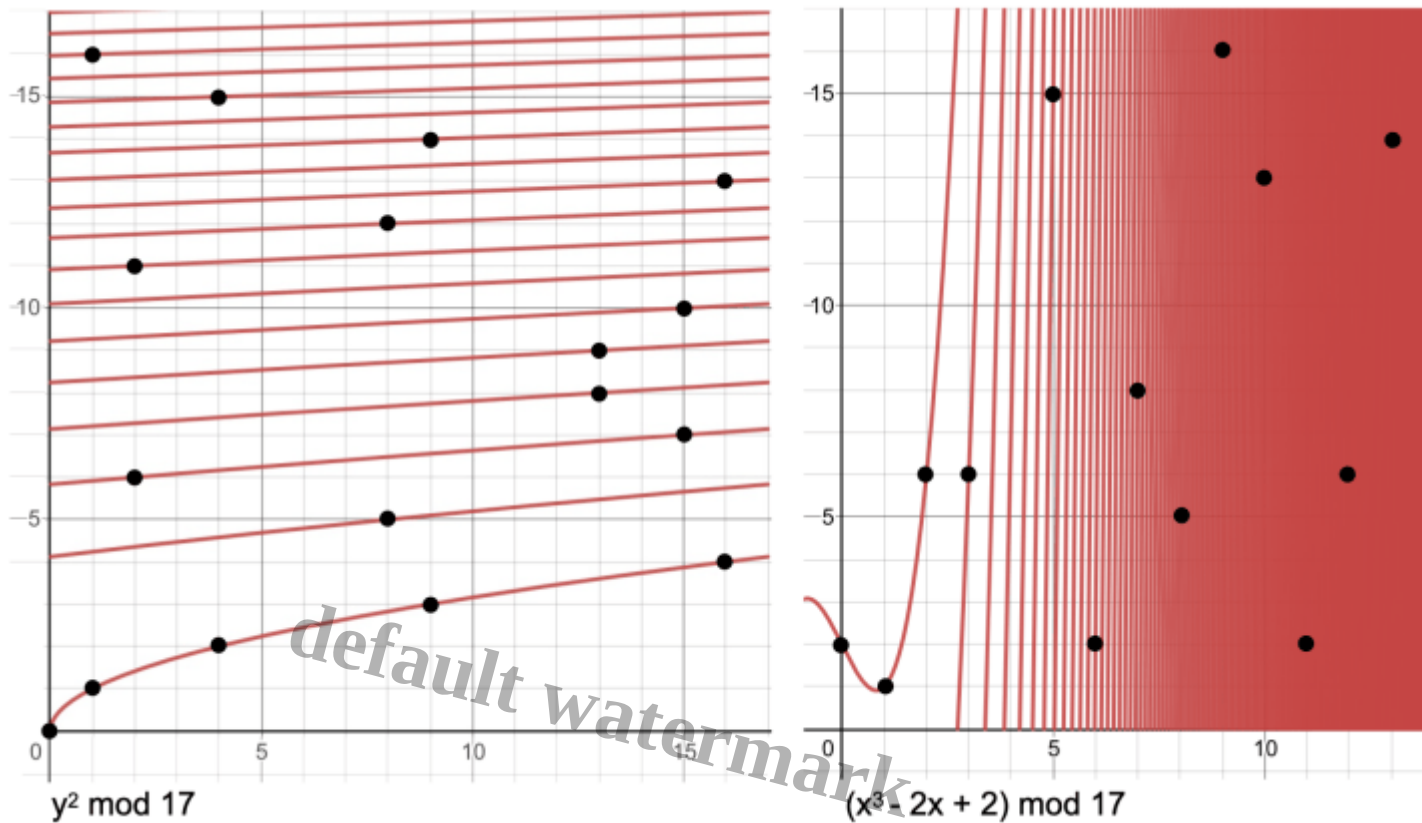
$$y^2 \bmod 17 = (x^3 - 2x + 2) \bmod 17$$

The **x** and **y** values that satisfy the equation will be different than in the case of the simple curve equation. Hereâ??s what the left and right sides look like drawn via the [Desmos Graphing Calculator](#) web utility.



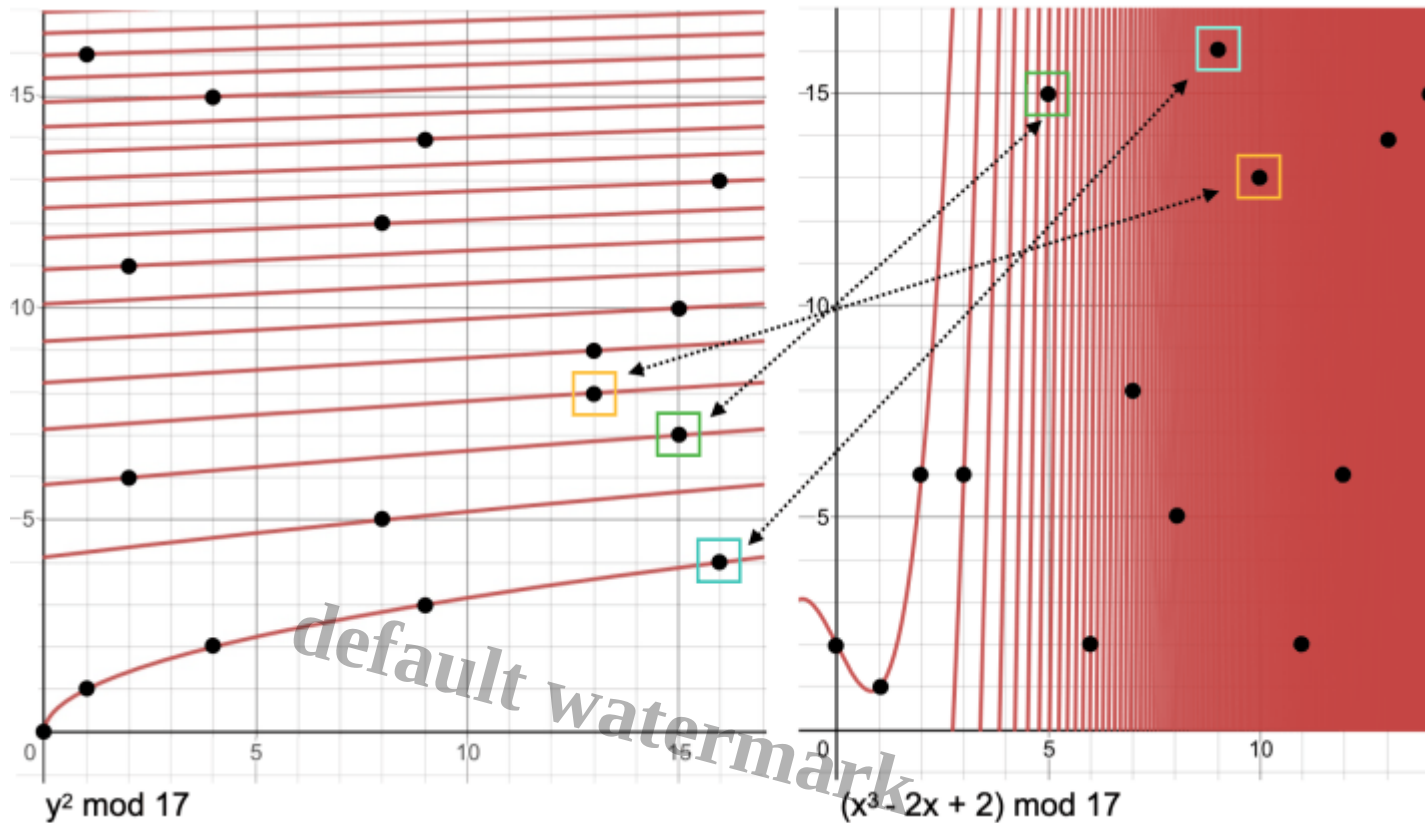
Finite fields

The graphs above show real numbers, i.e. include fractions. Mod calculations are useful for cryptography as they can deploy complex arithmetical operations that are always integers. 30 divided by 17 produces a real number 1.765, but $30 \bmod 17$ is the integer 13. The mod of two integers added or multiplied is always an integer. The graph here shows the integer values for the left and right side of the equation $y^2 \bmod 17 = (x^3 - 2x + 2) \bmod 17$.



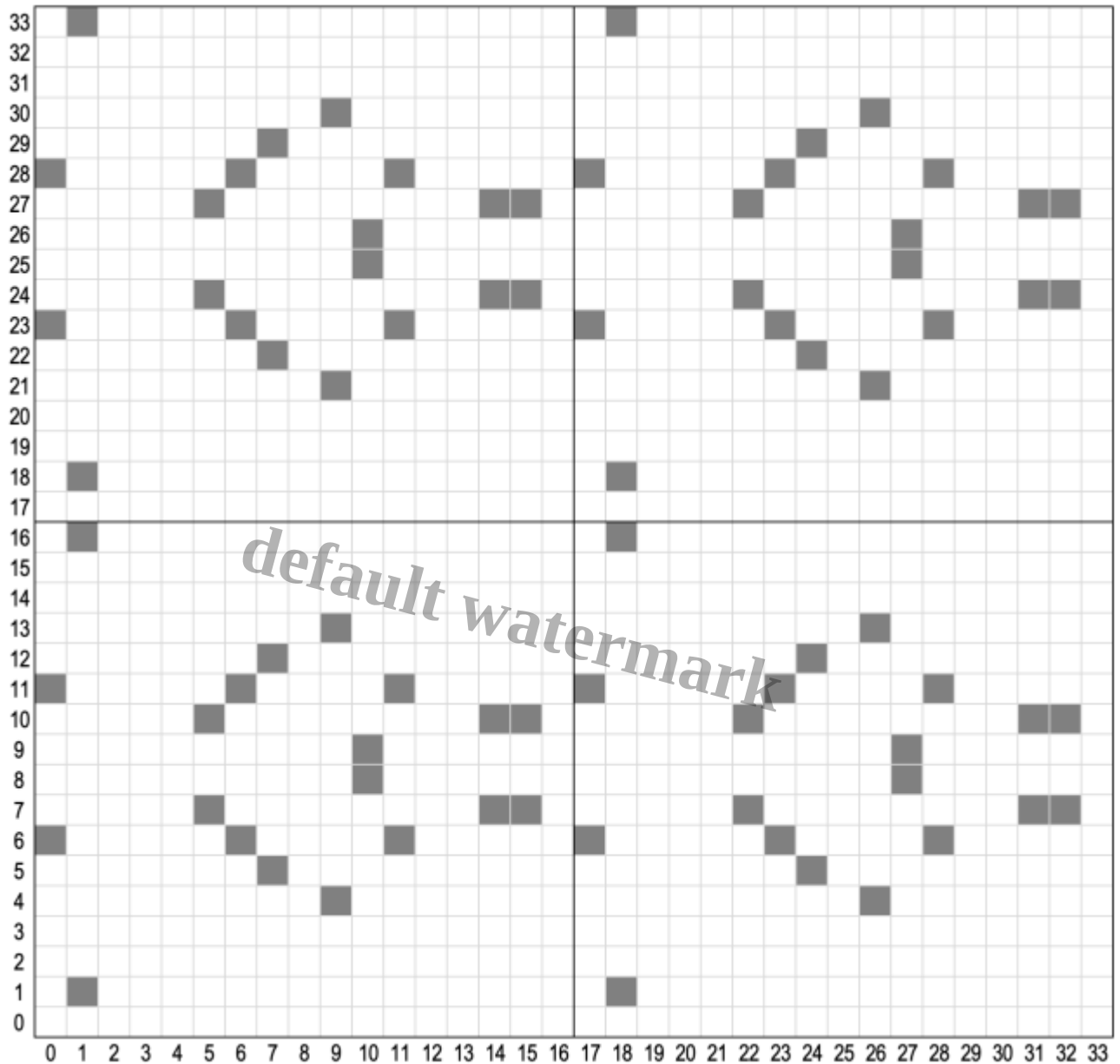
The *vertical* axis on the left graph shows y values. The *horizontal* axis on the left graph are the results of the $y^2 \bmod 17$ calculation. The *horizontal* axis of the right graph shows x values. The result of the $(x^3 - 2x + 2) \bmod 17$ calculation are on the *vertical* axis.

Iâ??ve identified 3 arbitrary points on the left graph that yield the same results as 3 points on the right graph. The correspondences so established are shown with arrows in the graphs below. So if $x = 10$ and $y = 8$ that yields $13 = 13$ via the formula. The full set of (x, y) points for which the formula holds true are $(0, 6)$, $(0, 11)$, $(1, 1)$, $(1, 16)$, $(5, 7)$, $(5, 10)$, $(6, 6)$, $(6, 11)$, $(7, 5)$, $(7, 12)$, $(9, 4)$, $(9, 13)$, $(10, 8)$, $(10, 9)$, $(11, 6)$, $(11, 11)$, $(14, 7)$, $(14, 10)$, $(15, 7)$, $(15, 10)$.



The grey squares in the chart below are the values for x and y where the left and right sides of the equation give the same integer value. I produced the chart via an Excel spreadsheet. I set it up to calculate for values for the x and y of each cell to find out whether $(x^3 - 2x + 2) \bmod 17$ has the same value as $y^2 \bmod 17$. For examples, the cell $x = 5, y = 4$ yields $16 \neq 1$. So that cell is not coloured. The cell $(5, 7)$ yields $15 = 15$. So cell $(5, 7)$ is coloured.

Calculations involving x and y beyond the mod value of 17 keep repeating. I've shown 4 repetitions here, but the chart extends indefinitely in either direction, including the negative direction. Only positive integer values are considered for x and y in this representation, as encryption usually only deploys positive integers. Note that due to this repetition the chart can be shown more economically as just one frame of dimensions 17×17 , i.e. the mod value. Note also that Each 17×17 grid frame is symmetrical about a horizontal axis.



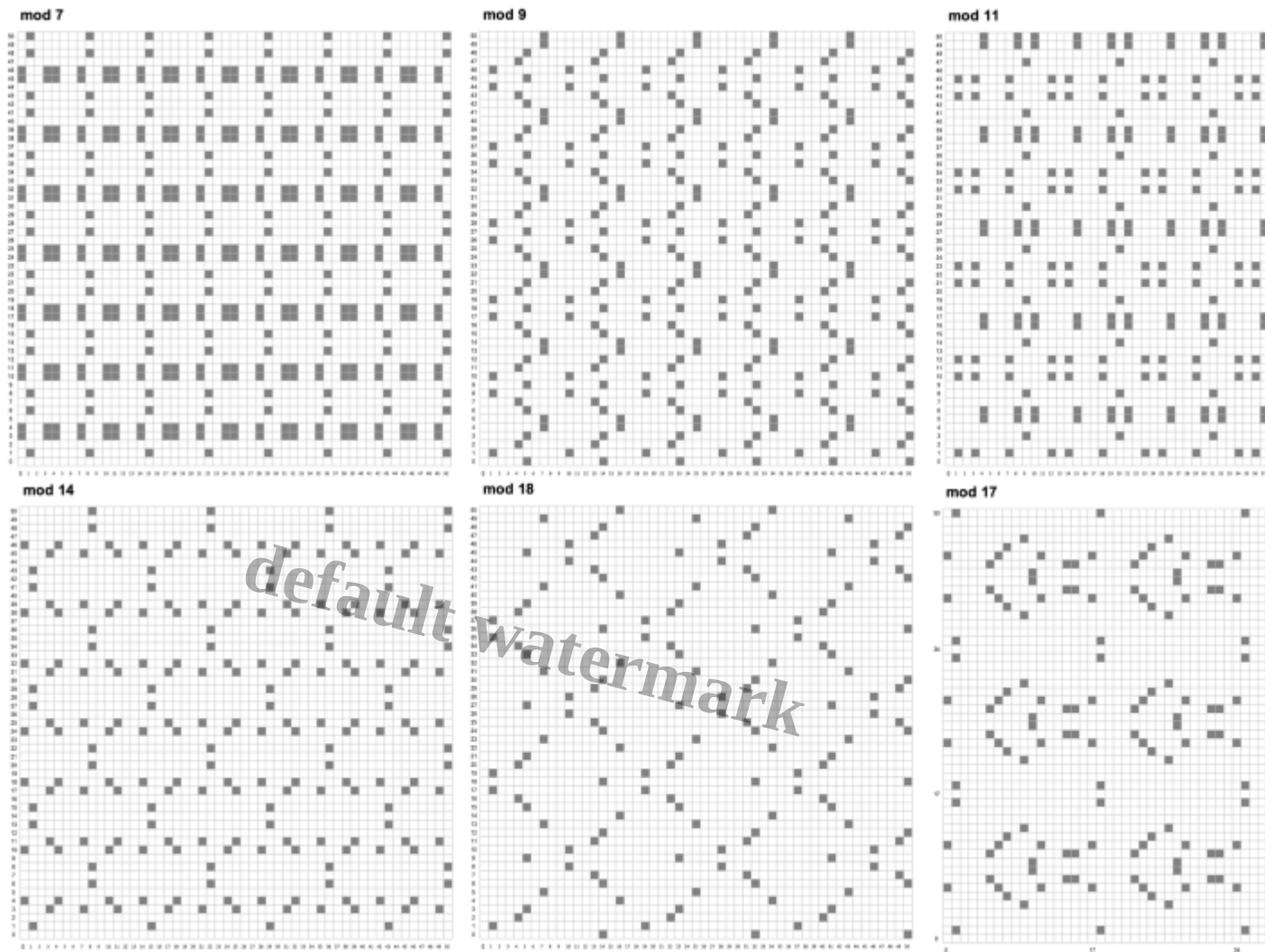
The interesting thing about the chart, described in standard texts as the **elliptic curve over a finite field**, is that it preserves some significant arithmetical properties of the elliptic curve such as arithmetical addition and scalar multiplication, while dealing only in integers.

I'll address this property and how it pertains to cryptography in the post that follows. In the mean time, I'll indulge my fascination with the spatial forms and diagrams for this kind of calculation.

The chart below shows the 2 values in the left and right of the equation for values of x and y for $y^2 \bmod 17 = (x^3 - 2x + 2) \bmod 17$ up to the value of 17. The equation is true only for the coordinates of the shaded cells.

16	1~2	1~1	1~6	1~6	1~7	1~15	1~2	1~8	1~5	1~16	1~13	1~2	1~6	1~14	1~15	1~15	1~3
15	4~2	4~1	4~6	4~6	4~7	4~15	4~2	4~8	4~5	4~16	4~13	4~2	4~6	4~14	4~15	4~15	4~3
14	9~2	9~1	9~6	9~6	9~7	9~15	9~2	9~8	9~5	9~16	9~13	9~2	9~6	9~14	9~15	9~15	9~3
13	16~2	16~1	16~6	16~6	16~7	16~15	16~2	16~8	16~5	16~16	16~13	16~2	16~6	16~14	16~15	16~15	16~3
12	8~2	8~1	8~6	8~6	8~7	8~15	8~2	8~8	8~5	8~16	8~13	8~2	8~6	8~14	8~15	8~15	8~3
11	2~2	2~1	2~6	2~6	2~7	2~15	2~2	2~8	2~5	2~16	2~13	2~2	2~6	2~14	2~15	2~15	2~3
10	15~2	15~1	15~6	15~6	15~7	15~15	15~2	15~8	15~5	15~16	15~13	15~2	15~6	15~14	15~15	15~15	15~3
9	13~2	13~1	13~6	13~6	13~7	13~15	13~2	13~8	13~5	13~16	13~13	13~2	13~6	13~14	13~15	13~15	13~3
8	13~2	13~1	13~6	13~6	13~7	13~15	13~2	13~8	13~5	13~16	13~13	13~2	13~6	13~14	13~15	13~15	13~3
7	15~2	15~1	15~6	15~6	15~7	15~15	15~2	15~8	15~5	15~16	15~13	15~2	15~6	15~14	15~15	15~15	15~3
6	2~2	2~1	2~6	2~6	2~7	2~15	2~2	2~8	2~5	2~16	2~13	2~2	2~6	2~14	2~15	2~15	2~3
5	8~2	8~1	8~6	8~6	8~7	8~15	8~2	8~8	8~5	8~16	8~13	8~2	8~6	8~14	8~15	8~15	8~3
4	16~2	16~1	16~6	16~6	16~7	16~15	16~2	16~8	16~5	16~16	16~13	16~2	16~6	16~14	16~15	16~15	16~3
3	9~2	9~1	9~6	9~6	9~7	9~15	9~2	9~8	9~5	9~16	9~13	9~2	9~6	9~14	9~15	9~15	9~3
2	4~2	4~1	4~6	4~6	4~7	4~15	4~2	4~8	4~5	4~16	4~13	4~2	4~6	4~14	4~15	4~15	4~3
1	1~2	1~1	1~6	1~6	1~7	1~15	1~2	1~8	1~5	1~16	1~13	1~2	1~6	1~14	1~15	1~15	1~3
0	0~2	0~1	0~6	0~6	0~7	0~15	0~2	0~8	0~5	0~16	0~13	0~2	0~6	0~14	0~15	0~15	0~3
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16

The following charts show the patterns produced by using different mod divisors. They remind me of cellular automator diagrams, and perhaps suggest the potential for hidden messages, though Iâ??ll explain the mechanism next time.



The algebra of mod calculations is not entirely intuitive, especially translating elliptic curves to a finite field. I'm happy to be corrected on any of this.

Bibliography

- Grau, Sascha. 2017. Elliptic Curves over Finite Fields. Available online: <https://grau.de/code/elliptic2/> (accessed 12 May 2021).
- Raedy, Will. 2017. Elliptic Curve Cryptography Tutorial â?? Understanding ECC through the Diffie-Hellman Key Exchange. *Fullstack Academy*, 8 August. Available online: <https://www.youtube.com/watch?v=gAtBM06xwaw> (accessed 9 May 2021).

Category

1. Architecture

Tags

1. elliptic

2. encryption

Date Created

June 12, 2021

Author

rcoyne99

default watermark