Counting Points on Curves over Finite Fields

The project lets you experiment with numbers of solutions of an equation in two variables over a finite field.

Let $\mathbb{F}_q$ denote a finite field with q elements with $q = p^m$ with p prime. We look at solutions of equations in two variables (or three) and do heuristics by computer and try to find formulas for the number of these.

Example 1. Consider the equation $y^2 + y = x^3 + 1$ over $\mathbb{F}_2$. Let $N_n = \#\{(x, y) : x, y \in \mathbb{F}_{2^n} : y^2 + y = x^3 + 1\} + 1$. Calculate N_1, N_2, N_3 and so on. Can you find experimentally a formula for N_n ? Try first odd n.

Example 2. Consider the equation $x^3 + y^3 + z^3 = 0$ in projective space $\mathbb{P}^2$ over the field $\mathbb{F}_p$. (That is, we only look at $(x, y, z) \neq (0, 0, 0)$, and (x, y, z) and (cx, cy, cz) with $0 \neq c \in \mathbb{F}_p$ are considered the same.) Find experimentally a formula for the number of solutions for $p \equiv 2 \pmod 3$. That is, find for fixed prime $p \equiv 2 \pmod 3$

$$\#\{(0, 0, 0) \neq (x, y, z) : x, y, z \in \mathbb{F}_p : x^3 + y^3 + z^3 = 0\}/(p - 1)\,.$$

(Can you prove the formula that you guessed?) Then look at the case $p \equiv 1 \pmod 3$. How does the answer for $p \equiv 1 \pmod 3$ differ from the answer for $p \equiv 2 \pmod 3$? Try to do heuristics.

Example 3. As in Example 2 consider now the equation $x^3y + y^3z + z^3x = 0$ in projective space $\mathbb{P}^2$, but now over $\mathbb{F}_2$. Let

$$N_n = \frac{1}{2^n - 1}\#\{(0, 0, 0) \neq (x, y, z) : x, y, z \in \mathbb{F}_{2^n} : x^3y + y^3z + z^3x = 0\}\,.$$

Find N_1, N_2, N_3 and so on. Find a formula for N_k for the case that $k \not\equiv 0 \pmod 3$. For $k \equiv 0 \pmod 3$ write $N_{3k} = (2^{3k} + 1) - a_k$. Can you express a_{k+2} as a linear combination of a_k and a_{k+1}? Find a general formula (recursive relation).

Example 4. Consider the equation $y^2 + y = x^5 + 1$ over $\mathbb{F}_2$. Let $N_n = \#\{(x, y) \in \mathbb{F}_{2^n} : y^2 + y = x^5 + 1\} + 1$. Find N_1, N_2, N_3 and so on. Can you find a recursive relation for the numbers $a_k = N_k - (2^k + 1)$? Or a closed formula for the N_k ?

Example 5. Consider the equation $y^2 + y = x^3 + x + 1$ over $\mathbb{F}_2$. Let $N_n = \#\{(x, y) : x, y \in \mathbb{F}_{2^n} : y^2 + y = x^3 + x + 1\} + 1$. Calculate N_n for $n = 1, 2, \ldots$. Find an algebraic number α such that $N_n = 2^n + 1 - \alpha^n - \bar{\alpha}^n$. What is the absolute value of α?

Example 6. Go back to Example 2. Can you find an algebraic number α of absolute value p such that $N_n = p^n + 1 - \alpha^n - \bar{\alpha}^n$ for $p = 7$? And for $p = 13$? And in general? Which upper and lower bound does it give for N_n ?

Example 7. Consider now $y^2 + y = x^5 + 1$ over $\mathbb{F}_2$. Let $N_n = \#\{(x, y) : x, y \in \mathbb{F}_{2^n} : y^2 + y = x^5 + 1\} + 1$. Calculate N_n for $n = 1$ and $n = 2$. Find algebraic numbers α_1, α_2 of absolute value 2 such that $N_n = 2^n + 1 - \alpha_1^n - \bar{\alpha}_1^n - \alpha_2^n - \bar{\alpha}_2^n$ for $n = 1, 2$. Does this formula hold for $n > 2$?

Example 8. Try to do as in Example 7, but now for $y^2 + y = x^7$ over $\mathbb{F}_2$. Calculate N_1, N_2, N_3, etc. Can you find α_1, α_2 ? If not, with how many α does it work?

NOW YOU CAN EXPERIMENT!