Elliptic curves over a finite field

For building cryptosystems, we take the set of solutions of the elliptic curve equation over a finite field $\mathbb{F}_q$ with $q = p^r$ elements, where p is a prime number and r is a natural number. This is what we call the elliptic curve over $\mathbb{F}_q$. We assume $p > 3$, then the elliptic curve equation is the same as for infinite fields: $y^2 = x^3 + ax + b$.

At most $2q+1$ points are on this curve.

$$\chi_q : \mathbb{F}_q \longrightarrow \{-1, 1, 0\}, \quad x \longmapsto \begin{cases} 0 & \text{for } x \equiv 0 \bmod q \\ 1, & x \text{ has a square root in } \mathbb{F}_q \\ -1, & x \text{ has no " " " "}. \end{cases}$$

If $q = p$,

$$\chi_p : x \longmapsto x^{\frac{p-1}{2}} \bmod p.$$

Example: $\mathbb{F}_{11}$.

1^2	2^2	3^2	4^2	5^2
1	4	9	5	3

mod 11

quadratic residues

$6 \equiv -5$, $7 \equiv -4$, $8 \equiv -3$, $9 \equiv -2$, $10 \equiv -1 \bmod 11$. Non-residues: 2, 6, 7, 8, 10.

$N :=$ (number of points on the elliptic curve over $\mathbb{F}_q$).

$$N = 1 + \sum_{x \in \mathbb{F}_q} \left(1 + \chi_q(x^3 + ax + b)\right) = q + 1 + \sum_{x \in \mathbb{F}_q} \chi_q(x^3 + ax + b).$$

Hasse's Theorem: $|N - (q+1)| \leq 2\sqrt{q}$.

Example. The curve $y^2 = x^3 - x$ over $\mathbb{F}_{71}$

$\chi_{71}((-x)^3-(-x)) = \chi_{71}(-1)\cdot\chi_{71}(x^3-x)$

and $\chi_{71}(-1) = -1$. (71 is prime) $\Rightarrow N = q+1 = 72$.

Roots of $x^3 - x = x(x-1)(x+1)$:

Three points on the curve.

$x_1 = 1$, $y_1 = \sqrt{x_1^3 - x_1} = 0$, point of order 2:

$(x_1,y_1) + (x_1,y_1) =: (x_3,y_3)$, $= 2(x_1,y_1)$

$$x_3 = \left(\frac{3x_1^2+a}{2y_1}\right)^2 - 2x_1 = \left(\frac{3+(-1)}{2\cdot 0}\right)^2 - 2 = \infty$$

$$y_3 = -y_1 + \frac{3x_1^2+a}{2y_1}(x_1 - x_3) = \infty \Rightarrow (x_3,y_3) = \mathcal{O}.$$

Exercise. Check the order of the other two points obtained from the roots.

Points P of order 3: $2P = -P \Rightarrow x_3 = x_1$

$$\Rightarrow \left(\frac{3x_1^2-1}{2y_1}\right)^2 - 2x_1 = x_1 \Rightarrow (3x_1^2-1)^2 = 12x_1y_1^2$$

$$= 12x_1^4 - 12x_1^2$$

$\Rightarrow 3x_1^4 - 6x_1^2 - 1 = 0$. At most four roots for this in $\mathbb{F}_{71}$. $\Rightarrow$ At most eight points of order 3.

$x^3 - x$ quadratic residue in $\mathbb{F}_{71} \Rightarrow (-x)^3 - (-x)$ non-residue.

$\Rightarrow$ At most four points of order 3.

Finitely generated Abelian groups

Definition. A **group** is a set G together with a binary operation

$$G \times G \longrightarrow G$$
$$(a, b) \longmapsto a \text{ "+" } b.$$

This operation "+" must have the following properties:

- **Associativity.** For all a, b, c in G,
$$(a+b)+c = a+(b+c)$$
- **Existence of a neutral element.** There is $\mathcal{O}$ in G such that for all a in G: $\mathcal{O}+a = a = a+\mathcal{O}$.
- **Existence of inverses.** For each a in G, there exists an element $(-a)$ in G, such that
$$a+(-a) = \mathcal{O} = (-a)+a.$$

Definition. An **Abelian group** is a group G such that for all a, b in G, $a+b = b+a$.

Definition. A **set of generators** for a group G is a collection of elements $a_1, a_2, \dots, a_k \in G$ such that every element $x \in G$ can be written as

$$x = m_1 a_1 + m_2 a_2 + \dots + m_k a_k, \quad m_1, m_2, \dots, m_k \in \mathbb{Z},$$

$$m_1 a_1 := \underbrace{a_1 + a_1 + \dots + a_1}_{m_1 \text{ times}}, \quad -m_1 a_1 = m_1(-a_1).$$

If G has a finite set of generators, then it is called a **finitely generated group**.

The group structure of an elliptic curve

On the elliptic curve $y^2 = x^3 - x$ over $\mathbb{F}_{71}$, we have found 72 points, three of them of order 2 and at most four of order 3.

Classification Theorem for finitely generated Abelian groups G:

$$G \simeq \mathbb{Z}^r \times C_{p_1}^{r_1} \times C_{p_2}^{r_2} \times C_{p_3}^{r_3} \times \dots \times C_{p_n}^{r_n}$$

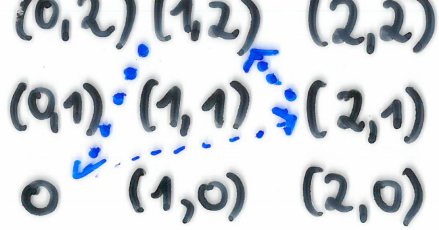
where C_q is the cyclic group with q elements, $p_1, p_2, \dots, p_n$ prime and $r_1, r_2, \dots, r_n \in \mathbb{N}$.

For finite groups, the rank r is zero.

So, an Abelian group of order $72 = 8 \cdot 9 = 2^3 \cdot 3^2$ must be a Cartesian product of

- a 2-torsion group of order 8: C_8, $C_4 \times C_2$ or $C_2 \times C_2 \times C_2$
- and a 3-torsion group of order 9: C_9 or $C_3 \times C_3$.

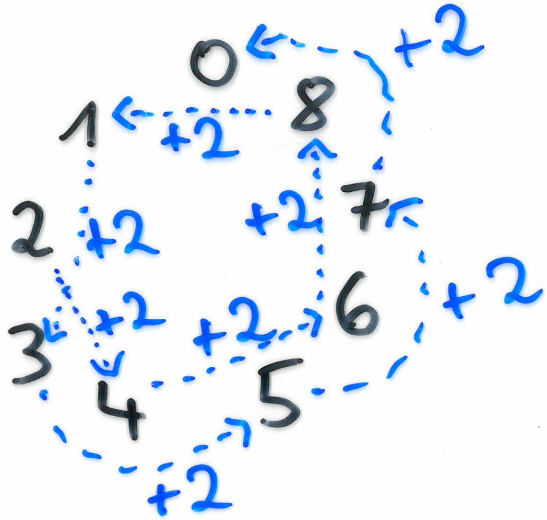
$C_3 \times C_3$:



eight elements of order 3:

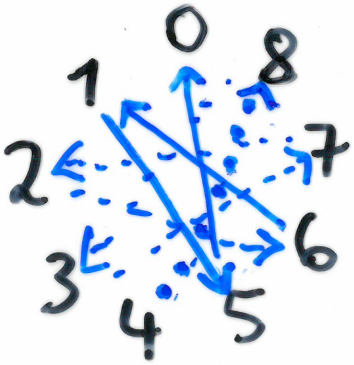
$3 \cdot (2,1) = 2 \cdot (2,1) + (2,1)$
$= (1,2) + (2,1) = (3,3) \equiv 0.$

C_9:



Order (2) = 9

2 mod 9



4 mod 9

Order (4) = 9

The order of the elements which are relatively prime to 9, i.e. 1, 2, 4, 5, 7, 8 is 9.

Elements of order 3: 3, and 6 mod 9.

$3 \cdot 3 = 9 \equiv 0$, $3 \cdot 6 = 18 \equiv 0 \bmod 9$.