Cubic curves over finite fields

E. Mazzoni and M. Schiltknecht

27th October 2020

1 Rational points over finite fields

In this talk we will study cubic equations over a finite field, namely the field $\mathbb{F}_p$ of the integers modulo p, and we will follow Chapter 4 of Silverman and Tate [1]. Consider a prime number p and a polynomial $F(x, y) \in \mathbb{F}_p[x, y]$ with coefficients in $\mathbb{F}_p$, defining a curve

$$C : F(x, y) = 0.$$

We can look for solutions of this equation in $\mathbb{F}_{p^n}$, an extension field of $\mathbb{F}_p$ with p^n elements.

Definition 1.1. *A point $(x, y) \in \mathbb{F}_p \times \mathbb{F}_p$ with $F(x, y) = 0$ is called a rational point of the curve C. We denote the set of all rational points of C by $C(\mathbb{F}_p)$.*

If C is a non-singular cubic curve, then we can define an addition law on it and the rational points of C, together with the point $\mathcal{O}$ at infinity, form an abelian group with this operation. The procedures and formulas that we have seen for cubic curves over $\mathbb{C}$ also work over $\mathbb{F}_p$. Since the field $\mathbb{F}_p$ is finite, there are also finitely many points which can lie on the curve C. Therefore $C(\mathbb{F}_p)$ is a finite group.

How can we find all rational points of the curve C? First of all, we should note that C will definitely contain the point $\mathcal{O}$ at infinity. For the other points, we know that they are of the form (x, y) for $x, y \in \mathbb{F}_p$. Since $\mathbb{F}_p \times \mathbb{F}_p$ is finite, we just need to check if $F(x, y) = 0$ for any possible choice of $x, y \in \mathbb{F}_p$.

2 The Hasse-Weil theorem

We will now consider the curve C given by

$$C : y^2 = f(x),$$

where $f \in \mathbb{F}_p[x]$ is a polynomial with coefficients in $\mathbb{F}_p$, and we will try to estimate the number of rational points of the curve C. To do this, the following proposition might be helpful:

Proposition 2.1. *Let $p \geq 3$ be a prime number. Then there are exactly $\frac{p-1}{2}$ non-zero elements of the field $\mathbb{F}_p$ which are squares (i.e. elements of the form x^2 for $x \in \mathbb{F}_p^*$).*

Consider $x \in \mathbb{F}_p$ and assume that $p \geq 3$. If $f(x) = 0$, there is a unique possibility for the vaue of y, namely $y = 0$. If $f(x) \neq 0$, we can distinguish two cases: either $f(x)$ is one of the $\frac{p-1}{2}$ squares of $\mathbb{F}_p$ and there are two possibilities for the value of y, or $f(x)$ is not a square in $\mathbb{F}_p$ and there are no solutions for y. Thus, if we assume that the values of $f(x)$ are randomly distributed among the elements of $\mathbb{F}_p$, we can estimate that the average number of solutions for each $x \in \mathbb{F}_p$ is about one. It turns out that for a separable polynomial $f \in \mathbb{F}_p[x]$ there is no tendency for the values assumed by f to be squares or non-squares. Therefore we can estimate that the total number of rational points of the curve C, including the point $\mathcal{O}$ at infinity, is about $p + 1$. This estimate can be formalized through the Hasse-Weil theorem, that we report from Silverman and Tate [1] on page 120.

Theorem 2.2 (Hasse-Weil)**.** *If C is a non-singular irreducible curve of genus g defined over a finite field $\mathbb{F}_p$, then the number of points on C with coordinates in $\mathbb{F}_p$ is equal to $p+1-\epsilon$, where ϵ satisfies $|\epsilon| \leq 2g\sqrt{p}$.*

The definition of genus does not fall within the scope of this presentation, hence we will only say that each curve $F(x,y)=0$ is associated with a non-negative number g, called its genus. In particular, any non-singular curve given by a cubic equation is a curve of genus 1. Therefore for an elliptic curve C over $\mathbb{F}_p$, we have the estimate

$$\Big||C(\mathbb{F}_p)| - (p+1)\Big| \leq 2\sqrt{p}.$$

3 A theorem of Gauss

Some special cases of the Hasse-Weil theorem had already been addressed by Gauss at the end of the 18th century. We will now give Gauss' proof of one of these special cases, the cubic Fermat curve $x^3+y^3=1$. We consider the curve in its homogeneous form

$$x^3+y^3+z^3=0$$

and its solutions in the projective sense. Hence we do not count the trivial solution $(0,0,0)$ and we identify a solution (x,y,z) with all of its non-zero multiples (ax,ay,az). Now we are ready to state Gauss's theorem, as we can find it in Silverman and Tate [1] on page 121.

Theorem 3.1 (Gauss)**.** *Let M_p be the number of projective solutions to the equation*

$$x^3+y^3+z^3=0$$

with x,y,z in the finite field $\mathbb{F}_p$.

(a) If $p \not\equiv 1 \pmod 3$, then $M_p = p+1$.

(b) If $p \equiv 1 \pmod 3$, then there exist integers A and B such that

$$4p = A^2 + 27B^2.$$

The numbers A and B are unique up to changing their signs, and if we fix the sign of A so that $A \equiv 1 \pmod 3$, then

$$M_p = p+1+A.$$

In order to prove Gauss' theorem, we need the following results (without proof).

Proposition 3.2. *Every line in the projective plane over the finite field $\mathbb{F}_p$ has exactly $p+1$ points.*

Definition 3.3. *Let $X,Y,Z \subset \mathbb{F}_p$ be subsets of $\mathbb{F}_p$. Then we denote by $[XYZ]$ the number of triples $(x,y,z) \in X \times Y \times Z$ with $x+y+z=0$.*

Proposition 3.4. *Let $X,Y,Z,W \subset \mathbb{F}_p$ be subsets of $\mathbb{F}_p$.*

(i) If $Z \cap W = \emptyset$, then $[XY(Z \cup W)] = [XYZ] + [XYW]$.

(ii) $\forall a \in \mathbb{F}_p^* : [XYZ] = [aX, aY, aZ]$.

(iii) $[XYZ] = [XZY] = [YXZ] = [YZX] = [ZXY] = [ZYX]$.

Proof of Gauss' theorem.

(a) We start by proving the first case, hence assume that $p \not\equiv 1 \ (mod\ 3)$.
Then 3 does not divide $p-1 = |\mathbb{F}_p^*|$. Since $\mathbb{F}_p^*$ is a cyclic group, it follows that the map

$$\Phi : \mathbb{F}_p^* \to \mathbb{F}_p^*,\ x \mapsto x^3$$

is a group isomorphism. Since $0^3 = 0$, we get that every element of $\mathbb{F}_p$ has a unique cubic root. Therefore the number of solutions of the equation

$$x^3 + y^3 + z^3 = 0$$

is equal to the number of solution of the linear equation

$$x + y + z = 0.$$

Since this equation defines a line in the projective plane over $\mathbb{F}_p$ and every such line has exactly $p+1$ points, it follows that there are $p+1$ projective solutions to the equation $x^3 + y^3 + z^3 = 0$. Therefore $M_p = p + 1$.

(b) Now assume that $p \equiv 1 \ (mod\ 3)$.
Then there exists $m \in \mathbb{N}$ with $p = 3m + 1$. Since 3 divides $p - 1 = |\mathbb{F}_p^*|$, the group homomorphism

$$\Phi : \mathbb{F}_p^* \to \mathbb{F}_p^*,\ x \mapsto x^3$$

is not surjective. Denote by $R = \{x^3 \mid x \in \mathbb{F}_p^*\}$ the image of Φ. R is a subgroup of $\mathbb{F}_p^*$ of index 3, thus the kernel of Φ consists of three elements $1, u, u^2$ for a $u \in \mathbb{F}_p^*$ with $u^3 = 1$. Therefore for any $x^3 \in R$ there are exactly 3 elements of $\mathbb{F}_p^*$, namely x, ux and u^2x, that give x^3 when cubed.

We can now determine the number of solutions M_p. We start by considering the solutions of $x^3 + y^3 + z^3 = 0$ with $x, y, z \neq 0$. With the notation introduced above, there are $[RRR]$ ways of writing zero as a sum of three non-zero cubes. For each non-zero cube, there are 3 elements of $\mathbb{F}_p^*$ which give that cube. Thus there are $3^3[RRR] = 27[RRR]$ solutions of $x^3 + y^3 + z^3 = 0$ such that $x, y, z \neq 0$. Since we are only interested in the projective solutions, we identify the solutions that are proportional, i.e. we identify a solution (x, y, z) with all of its multiples (ax, ay, az) with $a \in \mathbb{F}_p^*$. Since there are $|\mathbb{F}_p^*| = p - 1$ possible choices for a, the number of projective solutions of $x^3 + y^3 + z^3 = 0$ with $x, y, z \neq 0$ is

$$\frac{27[RRR]}{p-1} = \frac{9[RRR]}{m}.$$

Now we consider the solutions of $x^3 + y^3 + z^3 = 0$ with $z = 0$. Because we do not count the trivial solution $(0, 0, 0)$, x and y can not be zero. Hence we can choose any $x \in \mathbb{F}_p^*$ and then there are 3 possible values for y, namely $-x$, $-ux$ and $-u^2x$. Therefore there are $3|\mathbb{F}_p^*| = 3(p-1)$ solutions of $x^3 + y^3 + z^3 = 0$ with $z = 0$. By doing the same with $x = 0$ and then with $y = 0$, we can see

that there are $9(p-1)$ solutions of our equation with one coordinate equal to zero. As before, this results in

$$\frac{9(p-1)}{p-1} = 9$$

projective solutions with one coordinate zero. Therefore the total number of projective solutions of the equation $x^3 + y^3 + z^3 = 0$ is

$$M_p = \frac{9[RRR]}{m} + 9 = 9\left(\frac{[RRR]}{m} + 1\right).$$

Denote by S and T the other two cosets of R in $\mathbb{F}_p^*$, i.e. take $s \in \mathbb{F}_p^* \setminus R$ and let $S = sR = \{sr \mid r \in R\}$ and $T = s^2R = \{s^2r \mid r \in R\}$. Then

$$\mathbb{F}_p = \{0\} \cup R \cup S \cup T$$

is a disjoint union and $|R| = |S| = |T| = \frac{p-1}{3} = m$. Hence

$$[RR\{0\}] + [RRR] + [RRS] + [RRT] = [RR\mathbb{F}_p] = |R|^2 = m^2.$$

Since $[RRS] = [sR, sR, sS] = [SST]$ and $[RRT] = [s^2R, s^2R, s^2T] = [TTS]$, we get

$$[RR\{0\}] + [RRR] + [SST] + [TTS] = m^2. \tag{1}$$

Since $[\mathbb{F}_pTS] = |T| \cdot |S| = m^2$, we also have

$$[\{0\}TS] + [RTS] + [STS] + [TTS] = [\mathbb{F}_pTS] = m^2. \tag{2}$$

Note that $-1 = (-1)^3$ is a cube and therefore $R = -R$, $S = -S$ and $T = -T$. Since $(-S) \cap T = S \cap T = \emptyset$, $[\{0\}TS]$ must be 0. Since $-R = R$, we have $[RR\{0\}] = |R| = m$. Therefore by subtracting (2) from (1), we get

$$m + [RRR] = [RTS],$$

from which it follows that

$$M_p = 9\frac{[RTS]}{m}.$$

Let $\zeta = e^{2\pi i/p} \in \mathbb{C}$ and define

$$\alpha_1 = \sum_{r \in R} \zeta^r, \ \alpha_2 = \sum_{s \in S} \zeta^s, \ \alpha_3 = \sum_{t \in T} \zeta^t.$$

Claim 3.5. $\alpha_1 + \alpha_2 + \alpha_3 = -1$.

Proof. Since $\zeta^{p-1} + \zeta^{p-2} + ... + \zeta + 1 = \frac{\zeta^p - 1}{\zeta - 1} = 0$, we have that

$$\alpha_1 + \alpha_2 + \alpha_3 \ = \sum_{x \in R \cup S \cup T} \zeta^x = \sum_{x=1}^{p-1} \zeta^x = -1.$$

□ *(Claim)*

Claim 3.6. $\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3 = -m$.

Proof. We can write $\alpha_2\alpha_3$ as

$$\alpha_2\alpha_3 = \sum_{s\in S}\zeta^s \cdot \sum_{t\in T}\zeta^t \;\; = \sum_{s\in S,\, t\in T}\zeta^{s+t} = \sum_{x\in\mathbb{F}_p}[ST\{-x\}]\zeta^x,$$

where $[ST\{-x\}]$ is the number of pairs $(s,t)\in S\times T$ with $s+t=x$. Note that for any $r\in R$ we have

$$[ST\{-x\}] = [rS, rT, \{-rx\}] = [ST\{-rx\}]$$

and thus

$$m[ST\{-x\}] = \sum_{r\in R}[ST\{-rx\}] = [S,T,Rx] = \begin{cases}[STR] & \text{if } x\in R\\ [STS] & \text{if } x\in S\\ [STT] & \text{if } x\in T\end{cases}.$$

Define the integers a, b, c by

$$a = \frac{[STR]}{m},\; b = \frac{[STS]}{m},\; c = \frac{[STT]}{m}.$$

Then

$$\alpha_2\alpha_3 = \sum_{x\in\mathbb{F}_p}[ST\{-x\}]\zeta^x = \sum_{r\in R}a\zeta^r + \sum_{s\in S}b\zeta^s + \sum_{t\in T}c\zeta^t = a\alpha_1 + b\alpha_2 + c\alpha_3.$$

In the same way, we find that

$$\alpha_1\alpha_3 = a\alpha_2 + b\alpha_3 + c\alpha_1,$$

$$\alpha_1\alpha_2 = a\alpha_3 + b\alpha_1 + c\alpha_2.$$

Therefore

$$\begin{aligned}\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3 &= (a+b+c)(\alpha_1+\alpha_2+\alpha_3) = \\ &= -(a+b+c) = \\ &= -\left(\frac{[STR]}{m} + \frac{[STS]}{m} + \frac{[STT]}{m}\right) = \\ &= -\frac{[ST(R\cup S\cup T)]}{m} = \\ &= -\frac{[ST\mathbb{F}_p] - [ST\{0\}]}{m} = \\ &= -m.\end{aligned}$$

□ *(Claim)*

Claim 3.7. $\alpha_1^2 + \alpha_2^2 + \alpha_3^2 = 1 + 2m.$

Proof. By Claim 3.5 and Claim 3.6 it follows that

$$\alpha_1^2 + \alpha_2^2 + \alpha_3^2 = (\alpha_1+\alpha_2+\alpha_3)^2 - 2(\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3) = 1 + 2m.$$

□ *(Claim)*

Claim 3.8. $\alpha_1\alpha_2\alpha_3 = \frac{a+km}{3}$ *with* $k = 3a - m$.

Proof. Consider the equations

$$\begin{aligned}\alpha_1(\alpha_2\alpha_3) &= \alpha_1(a\alpha_1 + b\alpha_2 + c\alpha_3),\\ \alpha_2(\alpha_1\alpha_3) &= \alpha_2(a\alpha_2 + b\alpha_3 + c\alpha_1),\\ \alpha_3(\alpha_1\alpha_2) &= \alpha_3(a\alpha_3 + b\alpha_1 + c\alpha_2).\end{aligned}$$

By summing these equations and using Claim 3.6 and Claim 3.7 we get

$$\begin{aligned}3\alpha_1\alpha_2\alpha_3 &= a(\alpha_1^2 + \alpha_2^2 + \alpha_3^2) + (b+c)(\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3) =\\ &= a(1+2m) + (b+c)(-m) =\\ &= a + km,\end{aligned}$$

where $k = 2a - (b+c) = 3a - (a+b+c) = 3a - m$. □ *(Claim)*

Let $A = 3k - 2$ and $B = b - c$. Then $A \equiv 1 \ (mod\ 3)$ and

$$M_p = 9\frac{[RTS]}{m} = 9a = 3(k+m) = 3k + p - 1 = p + 1 + A.$$

We still need to prove that A and B are unique and satisfy $4p = A^2 + 27B^2$.

Consider the polynomial $f(t) = (t-\alpha_1)(t-\alpha_2)(t-\alpha_3) \in \mathbb{Z}[t]$. Using the claims above, we can write f as

$$\begin{aligned}f(t) &= (t-\alpha_1)(t-\alpha_2)(t-\alpha_3) =\\ &= t^3 - (\alpha_1+\alpha_2+\alpha_3)t^2 + (\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3)t - \alpha_1\alpha_2\alpha_3 =\\ &= t^3 + t^2 - mt - \frac{a+km}{3}.\end{aligned}$$

Denote by $Disc_f$ the discriminant of f. Then we can compute a square root of $Disc_f$ using the formulas above:

$$\begin{aligned}\sqrt{Disc_f} &= (\alpha_1-\alpha_2)(\alpha_1-\alpha_3)(\alpha_2-\alpha_3) =\\ &= \alpha_2\alpha_3(\alpha_2-\alpha_3) + \alpha_1\alpha_3(\alpha_3-\alpha_1) + \alpha_1\alpha_2(\alpha_1-\alpha_2) =\\ &= (a\alpha_1 + b\alpha_2 + c\alpha_3)(\alpha_2-\alpha_3) + (a\alpha_2 + b\alpha_3 + c\alpha_1)(\alpha_3-\alpha_1)\\ &\qquad + (a\alpha_3 + b\alpha_1 + c\alpha_2)(\alpha_1-\alpha_2) =\\ &= (b-c)(\alpha_1^2 + \alpha_2^2 + \alpha_3^2 - \alpha_1\alpha_2 - \alpha_1\alpha_3 - \alpha_2\alpha_3) =\\ &= (b-c)(1+3m) =\\ &= Bp.\end{aligned}$$

Let $\beta_i = 1 + 3\alpha_i$ for $i \in \{1,2,3\}$.
Then we have

$$\beta_1 + \beta_2 + \beta_3 = 3(\alpha_1+\alpha_2+\alpha_3+1) = 0,$$

$$\beta_1\beta_2 + \beta_1\beta_3 + \beta_2\beta_3 = 3 + 6(\alpha_1+\alpha_2+\alpha_3) + 9(\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3) = -3p,$$

$$\beta_1\beta_2\beta_3 = 1 + 3(\alpha_1+\alpha_2+\alpha_3) + 9(\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3) + 27\alpha_1\alpha_2\alpha_3 = Ap.$$

Define another polynomial $g(t) = (t-\beta_1)(t-\beta_2)(t-\beta_3) \in \mathbb{Z}[t]$. With the three equations above we can write g as

$$g(t) = t^3 - 3pt - Ap.$$

Denote the discriminant of g by $Disc_g$. From the formula for the discriminant of a cubic polynomial, it follows that

$$Disc_g = 4 \cdot 27p^3 - 27A^2p^2.$$

Since $\beta_i - \beta_j = 3(\alpha_i - \alpha_j)$, we must have $Disc_g = 27^2 Disc_f$. Thus

$$4 \cdot 27p^3 - 27A^2p^2 = 27^2B^2p^2,$$

and therefore

$$4p = A^2 + 27B^2.$$

Now let A' and B' be integers with $4p = A'^2 + 27B'^2$. Then

$$\begin{aligned} 4p(B'^2 - B^2) &= (A^2 + 27B^2)B'^2 - (A'^2 + 27B'^2)B^2 = \\ &= (AB' + A'B)(AB' - A'B). \end{aligned}$$

Hence p divides one of the two terms $(AB' + A'B)$ or $(AB' - A'B)$, so we can assume without loss of generality that $p \mid (AB' - A'B)$ (otherwise we can simply change the sign of A'). Consider the equation

$$\begin{aligned} 16p^2 &= (A^2 + 27B^2)(A'^2 + 27B'^2) = \\ &= A^2A'^2 + 27A'^2B^2 + 27A^2B'^2 + 27^2B^2B'^2 = \\ &= (AA' + 27BB')^2 + 27(AB' - A'B)^2. \end{aligned}$$

Since $p \mid (AB' - A'B)$, we get that

$$16 - \left(\frac{AA' + 27BB'}{p}\right)^2 = 27\left(\frac{AB' - A'B}{p}\right)^2.$$

It is clear that the left-hand side can be at most 16 and the right-hand side is 27 times the square of an integer, thus both sides must be zero and $AB' = A'B$. Define $\lambda = \frac{A'}{A} = \frac{B'}{B}$, then $A' = \lambda A$ and $B' = \lambda B$. Since

$$A'^2 + 27B'^2 = \lambda^2(A^2 + 27B^2) = \lambda^2(A'^2 + 27B'^2),$$

we have $\lambda \in \{-1, 1\}$. The conditions $A \equiv 1 \ (mod\ 3)$ and $A' \equiv 1 \ (mod\ 3)$ imply that $sign(A) = sign(A')$, hence $\lambda = 1$.
Therefore A and B are unique and the proof of Gauss' theorem is complete. $\square$

4 Points of Finite Order Revisited

For this part we will stick closely to section 3 in chapter IV of [1]. Consider

$$C\colon y^2 = x^3 + ax^2 + bx + c,$$

where $a, b, c \in \mathbb{Z}$ and let

$$\bar{C}\colon y^2 = x^3 + \bar{a}x^2 + \bar{b}x + \bar{c}$$

be the reduced curve C modulo p, where we have $\bar{k} \coloneqq k \bmod p$ for every $k \in \mathbb{Z}$. Suppose $(x, y) \in C(\mathbb{Z})$. Then x, y solve the equation for C. If we reduce the equation modulo p, we get

$$\bar{y}^2 = \bar{x}^3 + \bar{a}\bar{x}^2 + \bar{b}\bar{x} + \bar{c}.$$

Thus $(\bar{x}, \bar{y}) \in \bar{C}(\mathbb{F}_p)$.

Now let $\Phi \coloneqq \{P = (x, y) \in C(\mathbb{Q}) \mid P \text{ has finite order}\}$. We have already seen this object, it is precisely the torsion group, i. e. $\Phi = C(\mathbb{Q})_{\text{tors}}$. In particular Φ is a subgroup of $C(\mathbb{Q})$.

By the Nagell-Lutz theorem, the points of finite order have integer coordinates. So we can define a *reduction modulo p map*

$$\begin{aligned} \varphi\colon \Phi &\to \bar{C}(\mathbb{F}_p) \\ P \mapsto \bar{P} &= \begin{cases} (\bar{x}, \bar{y}) & \text{if } P = (x, y), \\ \bar{\mathcal{O}} & \text{if } P = \mathcal{O}. \end{cases} \end{aligned}$$

For $\bar{C}(\mathbb{F}_p)$ to be a group, we need that the reduced curve $\bar{C}$ is non-singular.

Lemma 4.1. *The reduced curve $\bar{C}$ is non-singular if and only if $p \nmid 2D$, where D is the discriminant of C.*

Proof. Note that if $p = 2$, we get rid of the equation for the partial derivative with respect to y, namely $2y = 0$, and we always get a singular point on $\bar{C}$, say $(s, t) \in \overline{\mathbb{F}_2}^2$, where s is chosen such that $3s^2 + 2\bar{a}s + \bar{b} = 0$ and t is so that $t^2 = s^3 + \bar{a}s^2 + \bar{b}s + \bar{c}$. If $p \geq 3$, then $2y = 0$ implies $y = 0$ and x needs to be a common root of $x^3 + \bar{a}x^2 + \bar{b}x + \bar{c}$ and its derivative. Thus x has to be a multiple root of $x^3 + \bar{a}x^2 + \bar{b}x + \bar{c}$. So in the case where $p \geq 3$, we see that $\bar{C}$ is non-singular if and only if $\bar{D} \neq 0$, where $\bar{D} = D \bmod p$ is the discriminant of $\bar{C}$. Now $\bar{D} \neq 0$ if and only if $p \nmid D$. Thus $\bar{C}$ is non-singular if and only if $p \neq 2$ and $p \nmid D$. Combined, we can also write these two conditions as $p \nmid 2D$. □

We now show that φ is a group homomorphism, i. e. $\overline{P + Q} = \bar{P} + \bar{Q}$. First note that

$$\overline{-P} = \overline{(x, -y)} = (\bar{x}, -\bar{y}) = -\bar{P}.$$

It suffices to show, that $P + Q + R = \mathcal{O}$ implies $\bar{P} + \bar{Q} + \bar{R} = \bar{\mathcal{O}}$, since for $R \coloneqq -(P + Q)$ we see that $\bar{P} + \bar{Q} + \bar{R} = \bar{\mathcal{O}}$ if and only if

$$\bar{P} + \bar{Q} = \bar{\mathcal{O}} - \bar{R} = -\bar{R} = \overline{-R} = \overline{P + Q}.$$

If without loss of generality $R = \mathcal{O}$, then $P + Q + R = \mathcal{O}$ implies $P = -Q$ and thus

$$\bar{P} + \bar{Q} + \bar{R} = \bar{P} + (\overline{-P}) = \bar{P} - \bar{P} = \bar{\mathcal{O}}.$$

Therefore we only need to show the statement for three non-trivial points $P_i = (x_i, y_i)$, where $i = 1, 2, 3$. We know that $P_1 + P_2 + P_3 = \mathcal{O}$ if and only if all three

points are on the same line. Let $y = \lambda x + \mu$ be the line through P_1, P_2, P_3. If all points coincide, take the tangent line. Use the explicit formula for the sum to get

$$x_3 = \lambda^2 - a - x_1 - x_2 \quad \text{and} \quad y_3 = \lambda x_3 + \mu.$$

Since $x_i, y_i, a \in \mathbb{Z}$, we see that $\lambda, \mu \in \mathbb{Z}$. Substitution yields

$$\begin{aligned} 0 &= x^3 + ax^2 + bx + c - (\lambda x + \mu)^2 \\ &= (x - x_1)(x - x_2)(x - x_3). \end{aligned}$$

If we reduce modulo p, we get

$$x^3 + \bar{a}x^2 + \bar{b}x + \bar{c} - (\bar{\lambda}x + \bar{\mu})^2 = (x - \overline{x_1})(x - \overline{x_2})(x - \overline{x_3}).$$

Reduction also yields $\overline{y_i} = \bar{\lambda}\overline{x_i} + \bar{\mu}$, for $i = 1, 2, 3$. Thus the line $y = \bar{\lambda}x + \bar{\mu}$ intersects $\bar{C}$ at $\bar{P}_i$ for all $i = 1, 2, 3$. Therefore $\bar{P}_1 + \bar{P}_2 + \bar{P}_3 = \bar{\mathcal{O}}$. So φ is indeed a group homomorphism. Moreover φ is injective, because a non-trivial element (x, y) gets sent to $(\bar{x}, \bar{y}) \neq \bar{\mathcal{O}}$.

We can now state the theorem that we just proved. The theorem can be found in [1] on page 123.

Theorem 4.2 (Reduction Modulo p Theorem)**.** *Let C be a non-singular cubic curve*

$$C\colon y^2 = x^3 + ax^2 + bx + c,$$

where $a, b, c \in \mathbb{Z}$ and let

$$D = -4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^2$$

be the discriminant. Let $\Phi \subseteq C(\mathbb{Q})$ be the torsion subgroup. If $p \nmid 2D$, then $\varphi\colon \Phi \hookrightarrow \bar{C}(\mathbb{F}_p)$ is an isomorphism of Φ onto a subgroup of $\bar{C}(\mathbb{F}_p)$.

Example 4.3. We now want to use the theorem to find points of finite order. Consider

$$C\colon y^2 = x^3 + 3.$$

We see that $D = -3^5$, so $p \nmid 2D$ if and only if $p \geq 5$. It's easy to check that

$$\bar{C}(\mathbb{F}_5) = \{\bar{\mathcal{O}}, (\bar{1}, \bar{2}), (\bar{1}, \bar{3}), (\bar{2}, \bar{1}), (\bar{2}, \bar{4}), (\bar{3}, \bar{0})\}.$$

Thus $|\bar{C}(\mathbb{F}_5)| = 6$. Analogously we get $|\bar{C}(\mathbb{F}_7)| = 13$. Using the theorem, once for $p = 5$ and once for $p = 7$, we see that $|\Phi|$ divides 6 and $|\Phi|$ divides 13. Therefore $|\Phi| = 1$ and $\Phi = \{\mathcal{O}\}$. So $\mathcal{O}$ is the only point of finite order in $C(\mathbb{Q})$.

Example 4.4. Consider

$$C\colon y^2 = x^3 + x.$$

Here the discriminant is $D = -2^2$, so to be able to use the theorem, we need $p \geq 3$. Checking all possibilities yields

$$\begin{aligned} \bar{C}(\mathbb{F}_3) &= \{\bar{\mathcal{O}}, (\bar{0}, \bar{0}), (\bar{2}, \bar{1}), (\bar{2}, \bar{2})\}, \\ \bar{C}(\mathbb{F}_5) &= \{\bar{\mathcal{O}}, (\bar{0}, \bar{0}), (\bar{2}, \bar{0}), (\bar{3}, \bar{0})\}. \end{aligned}$$

We know that a point in $\bar{C}$ has order two if and only if its y coordinate is zero. This implies

$$\bar{C}(\mathbb{F}_3) \cong \mathbb{Z}/4\mathbb{Z} \quad \text{and} \quad \bar{C}(\mathbb{F}_5) \cong \mathbb{F}_2 \oplus \mathbb{F}_2.$$

Now Φ can be seen as a subgroup of both of these groups. So either $|\Phi| = 1$ or $|\Phi| = 2$. Since $(0, 0) \in C(\mathbb{Q})$ has order two, we conclude that $\Phi = \{\mathcal{O}, (0, 0)\}$.

5 Reduction of an elliptic curve

For this section we will strongly stick to page 59 of [2]. Consider an elliptic curve

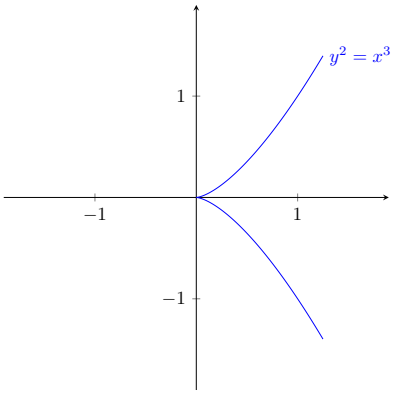
$$E\colon Y^2Z = X^3 + aXZ^2 + bZ^3,$$

where $a, b \in \mathbb{Q}$ and $D = 4a^3 + 27b^2 \neq 0$. By change of variables, we can assume $a, b \in \mathbb{Z}$ and $|D|$ is minimal. We then call such an equation *minimal*. Let

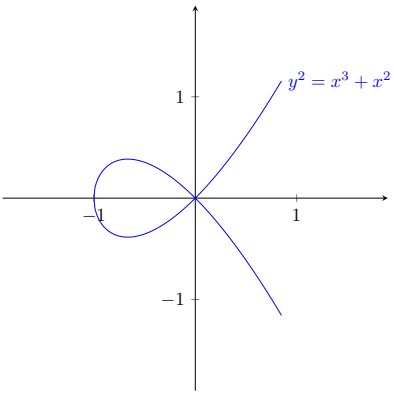
$$\bar{E}\colon Y^2Z = X^3 + \bar{a}XZ^2 + \bar{b}Z^3$$

be the reduction of E modulo p. There are certain cases to consider, namely

- *Good reduction* if $p \nmid 2D$, then $\bar{E}$ is an elliptic curve over $\mathbb{F}_p$.
- *Cuspidal (or additive) reduction* if $p \neq 2, 3$, $p \mid D$ and $p \mid (-2ab)$. Then $\bar{E}$ has a cusp.



- *Nodal (or multiplicative) reduction* if $p \neq 2, 3$, $p \mid D$ and $p \nmid (-2ab)$. Then $\bar{E}$ has a node.
  1. *split multiplicative reduction* if $-2ab$ is a square modulo p.
  2. *nonsplit multiplicative reduction* if $-2ab$ is not a square modulo p.



References

[1] J.H. Silverman and J.T. Tate, *Rational Points on Elliptic Curves*, Springer (1992).

[2] J.S. Milne, *Elliptic Curves*, BookSurge Publishers (2006).