Elliptic Curves and Public Key Cryptography (3rd VDS Summer School)

Discussion/Problem Session I

You are expected to at least read through this document before Wednesday's discussion session. Hopefully, you will also think about the exercises and work on those that appeal the most to you. I do not insist that you write down all of them because, although (with few exceptions) they are quite short, they may not be completely trivial if you have never thought about such things. On the other hand, if you are an algebraic-geometer only parts A and E may be new to you. In any case, be sure to understand what's going on in part B, the idea of rational function at the beginning of part C, and part E.2, because these will most probably be used on Thursday.

Given a field K, $\overline{K}$ denotes its algebraic closure.

A. Hill cypher keys

Let R be a commutative ring with 1 and $M_n(R)$ de ring of $n \times n$ with entries in R. Denote by $GL_n(R)$ the units in the latter ring, that is, matrices $A \in M_n(R)$ such that there exist $A^{-1} \in M_n(R)$ satisfying $AA^{-1} = A^{-1}A = I$. The following should be clear (perhaps after a little thought):

- $GL_n(R)$ with matrix multiplication is a group, called the *General Linear Group (of degree n over R).*
- Call $Ad(A)$ the matrix whose entry $Ad(A)_{ij}$ is the adjoint of the entry a_{ij} of A. The formula

  $$A \cdot Ad(A)^t = det(A) \cdot I = Ad(A)^t \cdot A$$

  is valid over any R.
- Hence, given $A \in M_n(R)$, $A \in GL_n(R) \iff det(A)$ is a unit (has a multiplicative inverse) in R.
- In particular, for any integer $N \geq 2$, $GL_n(\mathbb{Z}/N) = \{A \in M_n(\mathbb{Z}/N) : (det(A), N) = 1\}$.

Exercise 1. Call $\varphi_n(N) := |GL_n(\mathbb{Z}/N)|$ (observe that φ_1 is the usual Euler φ function).

(a) Find a formula for $\varphi_n(N)$ valid por any integers $n \geq 1, N \geq 2$. [SUGGESTION. Proceed like in standard proofs of the formula for $\varphi(N)$: show that φ_n is multiplicative ($\varphi_n(MN) = \varphi_n(M) \cdot \varphi_n(N)$ if $(M, N) = 1$); study the case $N = p$ prime ($\mathbb{Z}/p$ is a field); then look at $N = p^r$ and put everything together].

(b) Use your formula (and Sage or any other software that does exact arithmetic) to find how many different keys could Hill and Weisner use in their machines ($n = 6, N = 26$). Compare with the result given in class.

B. Projective plane / Projective space

At how many points do two different lines in a plane cross? In one, ... unless they are parallel. But in "real life", parallel lines, such as the two rails in a train track, also seem to meet at a point... in the horizon.

One of the advantages of working in the projective plane is that, by introducing a **line at infinity** ("the horizon") we can avoid exceptions in many geometrical results (and explain "perspective" much better, which in fact is, I believe, its historical origin).

Eventually K will be any field, but for now think of $K = \mathbb{R}$ to get a geometric picture.

Consider the affine plane $\mathbb{A}^2 = \{(x, y) : x, y \in K\}$. Put $\mathbb{A}^2$ inside $\mathbb{A}^3$ as "a horizontal plane at height 1", that is $\mathbb{A}^2 = \{(x, y, 1) : x, y \in K\} \subset \mathbb{A}^3$, and think of yourself (hopefully, you will soon see why) standing head-down on this plane so that your eye (only one, capable of looking in every direction) lies at the origin $(0, 0, 0) \in \mathbb{A}^3$.

Now, for any $P = (x, y, 1) \in \mathbb{A}^2$ there is exactly one "line of view" from your eye to P. Therefore, there is **almost** a bijection between points in $\mathbb{A}^2$ and lines in $\mathbb{A}^3$ going trough the origin.

I say "almost" because horizontal lines do not intersect $\mathbb{A}^2$. But in fact they do, **at infinity!**

Lets see this for the train tracks. Think of the right and left rails (parallel to the x-axis in this example) $R_r = \{(x,1,1) : x \in K\}, R_l = \{(x,-1,1) : x \in K\}$. The lines in $\mathbb{A}^3$ going through points in the rails have parametric equations, respectively, $L_r(t) = (tx,t,t), L_l(t) = (tx,-t,t)$, which, since I am looking at the horizon ($x \to \infty$, I can forget about $x = 0$), I prefer to write as $L_r(t) = (t,t/x,t/x), L_l(t) = (t,-t/x,t/x)$.

These lines are of course different when $x \in K$ (since $(x,1,1) \neq (x,-1,1)$), but when we let $x \to \infty$, they both become $(t,0,0)$, a line in $\mathbb{A}^3$ with direction vector $(1,0,0)$. This will be the point in the horizon towards which all lines in $\mathbb{A}^2$ parallel to the x-axis (that is, all horizontal lines) tend.

It is not hard to formalize this idea: given a field K, the *projective plane* over K, $\mathbb{P}^2_K$ if we need to keep track of the field, $\mathbb{P}^2$ otherwise, is the set of lines in $\mathbb{A}^3$ going trough the origin.

Notice that in our analogy, both rails of the train tracks meet at the same point at infinity, no matter whether we look East or West (take $x \to -\infty$). In other words, the East and West horizon get glued together (in some way).

Since a line in $\mathbb{A}^3$ is defined by its direction vector, which is unique up to multiplication by scalars, we now give a practical definition that introduces the so called *homogeneous coordinates*.

Definition. Let $(x,y,z),(x',y',z') \in \mathbb{A}^3$ be both $\neq (0,0,0)$. We say $(x,y,z) \sim (x',y',z') \iff$ there is a $\lambda \in K$, such that $(x,y,z) = \lambda(x',y',z')$. Since such λ is necessarily $\neq 0$, it is easy to see that $\sim$ is an equivalence relation. The *projective plane* over K is the quotient set

$$\mathbb{P}^2_K = \frac{\mathbb{A}^3_K \setminus \{0\}}{\sim}$$

- Points in $\mathbb{P}^2$ can be represented as $[x,y,z]$, with the remark that $[x,y,z] = [\lambda x, \lambda y, \lambda z]$. We will use this notation (that reminds us that they are equivalence classes), or sometimes $[x : y : z]$ (that, moreover, reminds us that there is a λ involved), to distinguish points in $\mathbb{P}^2$ from points in $\mathbb{A}^2$.
- We have $\mathbb{A}^2 \subset \mathbb{P}^2$ given by $(x,y) \to [x,y,1]$, and **should notice** that $[x,y,z] \in \mathbb{Z}^2 \iff z \neq 0$ (since then $[x,y,z] = [x/z, y/z, 1]$). But we could have chosen another coordinate to be 1 (or non-zero), and in fact we can see that $\mathbb{P}^2$ is covered by 3 copies of $\mathbb{A}^2$, the affine charts.
- $z = 0$ defines a line, that is called *the line at infinity* (of course "the" line is different if we look in a different affine chart).
- We can not evaluate polynomials $G \in K[x,y,z]$ at $P \in \mathbb{P}^2$, because the value $G(P)$ would not be independent of the chosen representative. But if G is **homogenous of degree** d then $G(\lambda x, \lambda y, \lambda z) = \lambda^d G(x,y,z)$ and, even if the actual value depends on λ, $G(P) = 0$ **is well defined**.

Definition. A plane projective algebraic curve (defined over K) is the set of points $P \in \mathbb{P}^2_K$ that satisfy $G(P) = 0$ for some homogeneous polynomial $G \in K[x,y,z]$. The *degree of the curve* is the degree of G. The curve is *irreducible* if G is irreducible. The points of the curve with $z = 0$ are the *points at infinity* of the curve.

- If we put $z = 1$ in the equation of a plane projective curve, we get a plane affine algebraic curve (we have deleted the points at infinity). This is called "dehomogenization" (or something similar; I hesitate to spell it even in Spanish!).
- Conversely, if we "homogonize" the equation of an affine curve by adding the right number of z's at each monomial, we get a projective curve (we have added the points at infinity).
- **Example:** The homogeneous equation $y^2z = x^3 + xz^2 + z^3$ gives the projectivization (projective completion) of the affine curve defined by $y^2 = x^3 + x + 1$.

Exercise 2. Work on any K, and remember that points may have coordinates in $\overline{K}$.

(a) Show that any curve (smooth or not) given by a Weierstraß equation $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ has a unique point $O = [0,1,0]$ at infinity.

(b) Show that any two distinct parallel lines $ax + by = c, ax + by = d$ meet at exactly one point in $\mathbb{P}^2$.

(c) [Here $char(K) \neq 2$. If you want, think of $K = \mathbb{R}, \overline{K} = \mathbb{C}$.] At how many points do the line at infinity $z = 0$ and the projectivization of the circle $x^2 + y^2 = R$ meet?

(d) [Here $char(K) \neq 2$. If you want, think of $K = \mathbb{R}, \overline{K} = \mathbb{C}$.] At how many points do the circles $x^2 + y^2 = 1$ and $x^2 + y^2 = 2$ meet in $\mathbb{P}^2$?

Items (b), (c) and (d) provide examples of the following important result.

Theorem (Bezout)**.** *Let C_1, C_2 be plane projective curves, of degrees d_1, d_2 respectively, with no common components (for example, C_1, C_2 are irreducible and $C_1 \neq C_2$). Then C_1 and C_2 intersect at $d_1 \cdot d_2$ points, counted with multiplicities.*

Exercise 3. We have just seen that C given by $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ has a unique point $O = [0, 1, 0]$ at infinity. Can you prove that this that not contradict the fact that, according to Bezout, C and the line at infinity, $z = 0$, should meet at 3 points?

- Projective spaces can be defined in the same way in any dimension: $\mathbb{P}^n$ are the lines going through the origin in $\mathbb{A}^{n+1}$.
- In other words,
$$\mathbb{P}^n_K = \frac{\mathbb{A}^{n+1}_K \setminus \{0\}}{\sim} = \frac{\{(x_0, x_1, \ldots, x_n) \neq 0\}}{\sim}$$
where $(x_0, x_1, \ldots, x_n) \sim (x'_0, x'_1, \ldots, x'_n) \iff (x_0, x_1, \ldots, x_n) = \lambda(x'_0, x'_1, \ldots, x'_n)$.
In this notation (one of the usual ones), $[x_0, x_1, \ldots, x_n]$ are the homogeneous coordinates and $x_0 = 0$ is the *hyperplane at infinity.*
- We will only look at $\mathbb{P}^2$ (projective plane) and $\mathbb{P}^1$ (projective line). To avoid confusion between the different y, we will use $[x, z]$ for the homogenous coordinates in $\mathbb{P}^1$, with $z = 0$ defining the *point at infinity.* We will call this point $\infty = [1, 0] \in \mathbb{P}^1$ to distinguish it from the point at infinity $O = [0, 1, 0] \in \mathbb{P}^2$ for elliptic curves.

Exercise 4. Do the following statements make sense to you?

(a) $\mathbb{P}^1_{\mathbb{R}}$ is homeomorphic to a circle S^1.

(b) $\mathbb{P}^1_{\mathbb{C}}$ is homeomorphic to a sphere S^2 (in fact, the Riemann sphere $\widehat{\mathbb{C}}$).

(c) $\mathbb{P}^2_K$ is $\mathbb{A}^2_K$ with a $\mathbb{P}^1_K$ glued at infinity.

C. Divisors and the Picard Group

Let C be a smooth projective algebraic curve defined over a field K.

- We will look at rational functions on C, that is, functions $f : C \to \overline{K} \cup \{\infty\}$ defined locally as a quotient of polynomials, $f = \frac{G}{H}$.
- G, H must be homogeneous of the same degree if we look at them in projective coordinates, so that
$$f([\lambda x, \lambda y, \lambda z]) = \frac{G(\lambda x, \lambda y, \lambda z)}{H(\lambda x, \lambda y, \lambda z)} = \frac{\lambda^d G(x, y, z)}{\lambda^d H(x, y, z)} = f([x, y, z]).$$
- Notice that such functions can have values in K, but also poles. **Example.**On $E : y^2 = x^3 - x$ the function $g = xz/y^2$ has $f((2, \sqrt{6})) = 1/3, f(\infty) = 0$ and a pole at $(1, 0)$, since $f((1, 0)) = 1/0 = \infty$.

- Notice also that, although this f seems not to be defined at $(0,0)$, this can be fixed using the equation of the curve:
$$f = \frac{xz}{y^2} = \frac{xz^2}{y^2 z} = \frac{xz^2}{x^3 - xz^2} = \frac{z^2}{x^2 - z^2} \rightsquigarrow f((0,0)) = f([0,0,1]) = 1$$

- The set of rational functions on C is a field, denoted by $\overline{K}(C)$. There is a function $0 \in \overline{K}(C)$ whose value is 0 on all $P \in C$. We will denote by $\overline{K}(C)^*$ the non-zero rational functions.

Definition. A *divisor* on C is a formal sum
$$D = \sum_{P \in C} n_P \, P$$
where $n_P \in \mathbb{Z}$ and only finitely many of them are not 0. (The idea is that D represents a finite set of points of C with multiplicities.)

- Divisors can be added: $(\sum_{P \in C} m_P \, P) + (\sum_{P \in C} n_P \, P) = \sum_{P \in C} (m_P + n_P) \, P$, and they clearly form a commutative group, $Div(C)$, where the neutral element is the 0 divisor ($n_P = 0 \, \forall P$). In fact, it is the free commutative group on the set of points of C.

- There is also an order on $Div(C)$: $D \geq 0 \iff n_P \geq 0 \, \forall P$; $D \geq D' \iff D - D' \geq 0$.

- The degree of a divisor is $deg(D) = \sum n_P$. The map $deg : Div(C) \longrightarrow \mathbb{Z}$ is a group homomorphism. We denote the subgroup of degree 0 divisors (the kernel of deg), by $Div^0(C)$.

- Given a rational function $f \in \overline{K}(C)^*$, we associate to it a divisor $div(f) = \sum_{P \in C} n_P \, P$, where n_P is *the order of f at P*. This means the following:

  - $n_P > 0 \iff f$ has a zero of order n_P at P.
  - $n_P < 0 \iff f$ has a pole of order $-n_P$ at P.
  - $n_P = 0 \iff f(P) \in \overline{K}$ and is not 0.
  - **Example:** The function $f = \frac{x^2(x-z)}{z^3}$ on $\mathbb{P}^1$ has divisor (the affine points are written in parenthesis so as to not confuse them with the multiplicities) $div(f) = 2(0) + (1) - 3\infty$

- Just as holomorphic functions on $\widehat{\mathbb{C}}$, functions $f \in \overline{K}(C)^*$ have the same number of zeroes and poles (counting multiplicities). In other words $deg(div(f)) = 0$. (For $C \subset \mathbb{P}^2$, a curve of degree d, a "proof" is as follows: $f = \frac{G}{H}$, with G, H homogeneous polynomials of the same degree e. The zeros of f are, except for cancellations, the intersection points of C and the curve $G = 0$, with multiplicities. The poles are, except for cancellations, the intersection points of C and the curve $H = 0$. By Bezout, both intersection divisors have degree de. Cancelling what must be cancelled, f has an equal number of zeroes and poles.)

Exercise 5. Prove that the set of *principal divisors*, $Prin(C) = \{div(f) : f \in \overline{K}(C)^*\}$, is a subgroup of $Div^0(C)$. Do not forget to check that $0 \in Prin(C)$.

Definition. The *Picard group of C* is the quotient group $Pic(C) = Div(C)/Prim(C)$. It is the class group of $Div(C)$ modulo the equivalence relation $D \sim D' \iff D - D' = div(f)$ for some rational function f. Two such divisors are said to be *linearly equivalent*.

Exercise 6. Prove

(a) If D and D' are linearly equivalent, then $deg(D) = deg(D')$.

(b) The linear equivalence classes of divisors of degree 0 form a subgroup of $Pic(C)$, denoted by $Pic^0(C)$.

(c) $Pic(C) = Pic^0(C) \oplus \mathbb{Z}$.

D. Riemann-Roch Theorem

Definition. Given a divisor $D \in Div(C)$, we associate to it the space of functions

$$\mathcal{L}(D) = \{f \in \overline{K}(C)^* : div(f) + D \geq 0\} \cup \{0\}.$$

Notice that the zero function is in $\mathcal{L}(D)$, but we will often "forget about it "when giving arguments or describing examples, such as the following.

- $div(f) \geq 0$ means f has no poles. Hence f must be constant. Thus, $\mathcal{L}(0) = \overline{K}^* \cup \{0\} = \overline{K}$.
- $div(f) + P \geq 0$ means f **may** have a single pole at P, **and no others**. Thus, constant functions are in $\mathcal{L}(P)$, but there may be others. In other words, $\mathcal{L}(0) \subseteq \mathcal{L}(P)$ and the inclusion may or not be an equality (see exercises 7 and 10 (a)).
- $div(f) - P \geq 0$ means f **must** have at least a single zero at P, and **can not** have poles. Since $deg(div(f)) = 0$ such an f does not exist. Hence, $\mathcal{L}(-P) = \{0\}$.
- As these examples show, the idea is that $\mathcal{L}(D)$ are functions with restrictions on the **possible poles** (coming from the positive part of D) and some **mandatory zeroes** (coming from the negative part of D).

Exercise 7. In the particular case $C = \mathbb{P}^1$, write for any $P \in \mathbb{P}^1$ (including $P = \infty$) a function with a simple pole at P and no others. Thus, $\mathcal{L}(0) \subsetneq \mathcal{L}(P)$.

Exercise 8. [Back to a general curve C] Prove that:

(a) $D \geq D' \Rightarrow \mathcal{L}(D') \subseteq \mathcal{L}(D)$.

(b) $deg(D) < 0 \Rightarrow \mathcal{L}(D) = \{0\}$.

(c) $\mathcal{L}(D)$ is a $\overline{K}$-vector space.

$\mathcal{L}(D)$ is finite dimensional (you do not have to prove this). Lets write $\ell(D) := dim_{\overline{K}}\mathcal{L}(D)$.

Theorem (Riemann-Roch)**.** *There exists a positive integer g (the **genus** of C) and a divisor K_C (**canonical divisor**) such that, for <u>any</u> $D \in Div(C)$,*

$$\ell(D) = deg(D) + 1 - g + \ell(K_C - D).$$

Exercise 9. Prove:

(a) $\ell(0) = 1$.

(b) $\ell(K_C) = g$.

(c) $deg(K_C) = 2g - 2$.

(d) $deg(D) > 2g - 2 \Rightarrow \ell(D) = deg(D) + 1 - g$.

E. Applications to Elliptic Curves

Remember that an elliptic curve over a (perfect) field K is a smooth projective curve E of genus $g = 1$, defined by (homogeneous) polynomials with coefficients in K, together with a point $P \in E(K)$. A priori, it is not a plane curve. We will make some comments on the field of definition, but for the exercises we will work over $\overline{K}$.

1. All elliptic curves are plane cubics and they can even be given in Weierstraß form.

Exercise 10. Let E be an elliptic curve, $O \in E$.

(a) Show that, given any $P \in E$, there does not exist a function $x \in \overline{K}(E)$ with a pole of order 1 at P and no other poles.

(b) Show that $\mathcal{L}(0) \subseteq \mathcal{L}(O) \subseteq \mathcal{L}(2\,O) \subseteq \mathcal{L}(3\,O) \subseteq \ldots$. Determine the dimensions of the spaces $\mathcal{L}(n\,O)$ for all integers $n \geq 0$.

(c) Show that there exists a function $x \in \overline{K}(E)$ with a pole of order 2 at O and no other poles. Show that there exists a function $y \in \overline{K}(E)$ with a pole of order 3 at O and no other poles.

(d) Prove that the functions x, y satisfy an equation of the form:

$$Ay^2 + a_1xy + a_3y = Bx^3 + a_2x^2 + a_4x + a_6, \quad a_i \in \overline{K}, A, B \in \overline{K}, A \neq 0, B \neq 0.$$

(e) Prove that there exist functions $x, y \in \overline{K}(E)$ that satisfy a Weierstraß equation:

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \quad a_i \in \overline{K}.$$

(f) If $char(K) \neq 2, 3$, prove that there exist functions $x, y \in \overline{K}(E)$ that satisfy a reduced Weierstraß equation:

$$y^2 = x^3 + Ax + B, \quad A, B \in \overline{K}.$$

(g) Explain why the map

$$\begin{aligned} \phi : E &\longrightarrow \mathbb{P}^2 \\ P &\longmapsto [x(P), y(P), 1] \end{aligned}$$

sends O to the point $[0, 1, 0] \in \mathbb{P}^2$.

With a little bit more of knowledge about morphisms of algebraic curves, it is not hard to prove that, if we call E' the **plane** algebraic curve defined by the Weierstraß equation, E' is smooth and the map ϕ above defines a curve isomorphism $E \simeq E'$. In particular, we can look at **any** elliptic curve as being given by a Weierstraß equation in $\mathbb{P}^2$ and $O = [0, 1, 0]$.

When E is defined over K and $O \in E(O)$, one can prove, using a natural action of the Galois group $Gal(\overline{K}/K)$ on $\mathcal{L}(D)$, that it is possible to take $a_i \in K$ in the Weierstraß equation, so that E' is also defined over K.

2. We can define a group structure on all elliptic curves

We have defined a geometric addition on elliptic curves given by Weirstaß equation, and we used Cayley-Bacharach to prove that it is associative. We want to define a group law on **any** elliptic curve (E, O), and do it in a way that is consistent with the geometric construction. To clarify notation, we will use $\oplus$ for addition on the elliptic curve, and $+$ for addition in $Pic(E)$.

Exercise 11. Consider the map

$$\begin{aligned} \kappa : E &\longrightarrow Pic^0(E) \\ P &\longmapsto \text{class of the divisor } P - O \end{aligned}$$

(a) Using Riemann-Roch, prove that κ is bijective. That is: $P - O \sim 0 \iff P = O$; given $D \in Div^0(E)$, there exists a (unique) $P \in E$ such that $D \sim P - O$.

(b) From the bijection, we can define an addition on E: $P \oplus Q := \kappa^{-1}(\kappa(P) + \kappa(Q))$. Convince yourself that this makes $(E, \oplus)$ into an additive group with O as neutral element.

(c) Prove that, if we start with E given by a Weierstraß equation and we take $O = [0, 1, 0] \in E$, the addition on E defined by the cords-and-tangents method coincides with the $\oplus$ we have have just defined and, therefore, is associative.