W. What is an elliptic curve

W.1. **The genus.** By definition, an *elliptic curve* over K is a projective planar irreducible curve C over K that contains at least one K-rational point and is of genus 1. What is the *genus*? Unfortunately, that is not so easy to explain. A complete formal definition goes beyond the scope of this text. Neverthelees, the ensuing comments might give an idea what the genus means.

If C is an irreducible curve over K, then the genus of C may be derived from the structure of $K(C)$. It somehow reflects properties of principal divisors. (If σ is a nonzero element of $K(C)$, then there are only finitely many places P with $v_P(\sigma) \neq 0$. The formal sum $\sum v_P(\sigma)P$ is called the principal divisor of σ.) Genus is always a nonnegative number and is usually denoted by g.

Since complex numbers may be identified with the euclidean plane, a planar curve over $K = \mathbb{C}$ may be regarded as a 2-dimensional object. Let us first ponder what kind of a 2-dimensional object the projective line $\mathbb{P}^1(\mathbb{C})$ should be associated with. The affine line $\mathbb{A}^1(\mathbb{C})$ coincides with the euclidean plane. The existence of the point at infinity changes, however, the picture completely. The proper 2-dimensional object to identify $\mathbb{P}^1(\mathbb{C})$ with is the sphere. This may be envisioned by considering a stereographic projection of a sphere to the euclidean plane, with the point at infinity being represented by the north pole of the sphere.

The sphere is an example of a closed 2-dimensional surface in the 3-dimensional real space. In this context the exact shape of the surface is not important. What is important are topological properties of the surface. It turns out that two such surfaces may be identified by continuous deformations if and only if they possess the same number of holes. A sphere has no hole. A toroid has one hole. The surface of a pretzel has two holes (going from doughnut to pretzel adds one hole). The number of holes is thus a topological invariant and this invariant is called the *genus* of the surface. This is how the notion of the genus of a curve arose. If C is a smooth irreducible projective planar curve over $\mathbb{C}$, then C forms a 2-dimensional structure that may be embedded into the 3-dimensional real space as a closed surface. The curve is of genus one if the surface to which it may be embedded has the shape of torus.

The existence of such an embedding has to be proved. That is done in topology and goes far beyond the scope of this text. Note however that such an embedding cannot be "seen" since the graph of the curve is a subset of $\mathbb{C} \times \mathbb{C}$, and thus it lives in a 4-dimensional real space. However, the fact that the surface of a complex elliptic curve forms a torus has certain consequences for elliptic curves over real numbers. When cutting a torus there appears either one ellipse or two of them. Because of that it may be expected that an elliptic curve over reals will have one or two closed branches.

Many authors define an elliptic curve as a projective irreducible curve of genus 1 that is smooth everywhere. This is a traditional approach that may be justified by the prominent role of smooth Weierstraß curves. These curves present a universal model of elliptic curves in the sense that whenever C is a curve of genus one that contains at least one K-rational point, then there exists a smooth Weierstraß curve E such that the function fields $K(C)$ and $K(E)$ are K-isomorphic (that is there exists an isomorphism that fixes each $\lambda \in K$.)

W.2. **Weierstraß curves.** An *affine Weierstraß curve* is the set C of all points $(\alpha_1, \alpha_2) \in \mathbb{A}^2$ that fulfil a *Weierstrass equation* $x_2^2 + x_2 g(x_1) = f(x_1)$, that is an equation in which $f, g \in K[x_1]$ are polynomials such that $\deg(g) \leq 1$, $\deg(f) = 3$, f is monic. It may be proved that the polynomial $x_2^2 + x_2 g(x_1) - f(x_1)$ is always irreducible. Each Weierstraß curve is thus an irreducible planar curve.

By convention, the coefficients of g are denoted by a_1 and a_3, and the coefficients of f by a_2, a_4 and a_6. The Weierstraß equation thus often appears in the *standard form*

$$x_2^2 + a_1x_1x_2 + a_3x_2 = x_1^3 + a_2x_1^2 + a_4x_1 + a_6.$$

Set $b_2 = 4a_2 + a_1^2$, $b_4 = 2a_4 + a_1a_3$, $b_6 = 4a_6 + a_3^2$ and

$$b_8 = 4a_2a_6 + a_2a_3^2 + a_1^2a_6 - a_4^2 - a_1a_3a_4.$$

It may be established that the curve C is smooth if and only if the *discriminant*

$$\Delta(C) = -8b_4^3 + 9b_2b_4b_6 - 27b_6^2 - b_2^2b_8$$

is different from 0.

Applications of Weierstraß curves usually assume that $\mathrm{char}(K) \notin \{2, 3\}$ and $a_1 = a_3 = 0$. Often it is also assumed that $a_2 = 0$. In those cases the smoothness of C correlates with the nonexistence of a multiple root of f. This will be now verified.

Suppose that $\mathrm{char}(K) \neq 2$ and that $C = V_w$, where $w(x_1, x_2) = x_2^2 - f(x_1)$. Then

$$\frac{\partial w}{\partial x_1} = -f'(x_1) \text{ and } \frac{\partial w}{\partial x_2} = 2x_2.$$

A point $(\alpha_1, 0) \in \mathbb{A}^2$ belongs to C if and only if $f(\alpha_1) = 0$. All of this means that (α_1, α_2) presents a singularity of C if and only if $\alpha_2 = 0$ and α_1 is a root of both f and f'. We have proved:

Theorem W.1. *Let C be the Weierstraß curve over K, $\mathrm{char}(K) \neq 2$, determined by $x_2^2 = f(x_1)$, $f \in K[x_1]$ cubic and monic. Then C is smooth if and only if f is separable (i.e., possesses no multiple root).*

If $a_1 = a_2 = a_3 = 0$, then the Weierstraß equation will often be written as $x_2^2 = x_1^3 + ax_1 + b$ or $y^2 = x^3 + ax + b$. The polynomial $x^3 + ax + b$ has multiple roots if and only $4a^3 + 27b^2 = 0$. The curve determined by $x_2^2 = x_1^3 + ax_1 + b$, $\mathrm{char}(K) \neq 2$, is thus smooth if and only if $4a^3 + 27b^2 \neq 0$.

This is the same condition as $4a_4^3 + 27a_6^2 \neq 0$. A mnemotechnical remark: Both terms of the sum may be expressed as $(i/2)^{i/2}a_i^{j/2}$, where $\{i, j\} = \{4, 6\}$.

Projective Weierstraß curves are obtained by homogenization. They are thus determined by equation

$$X_2^2X_3 + X_2G(X_1, X_3) = F(X_1, X_3), \text{ where } G(X_1, X_3) = a_1X_1X_3 + a_3X_3^2$$
$$\text{and } F(X_1, X_3) = X_1^3 + a_2X_1^2X_3 + a_4X_1X_3^2 + a_6X_3^3.$$

A point at infinity $(\alpha_1 : \alpha_2 : 0)$ belongs to the curve if and only if $0 = \alpha_1^3$. There is thus only one such point, and this point is equal to $(0 : 1 : 0)$.

Put $W(X_1, X_2, X_3) = X_2^2X_3 + X_2G(X_1, X_3) - F(X_1, X_3)$. Then

$$\frac{\partial W}{\partial X_1} = X_2\frac{\partial G}{\partial X_1} - \frac{\partial F}{\partial X_1},$$
$$\frac{\partial W}{\partial X_2} = 2X_2X_3 + G(X_1, X_3), \text{ and}$$
$$\frac{\partial W}{\partial X_3} = X_2^2 + X_2(a_1X_1 + 2a_3X_3) - \frac{\partial F}{\partial X_3}.$$

Hence $(\partial W/\partial X_1)(0, 1, 0) = 0 = (\partial W/\partial X_2)(0, 1, 0)$ and $(\partial W/\partial X_3)(0, 1, 0) = 1$. Each projective Weierstraß curve is therefore smooth at the point at infinity. An affine Weierstraß curve is thus smooth if and only if the corresponding projective Weierstraß curve is smooth.

As examples of affine Weierstraß curves consider curves over real numbers given by equations $x_2^2 = x_1^3 - c^3$ and $x_2^2 = x_1^3 - c^2x_1$. The former curve has a single

branch. In the central part it has a form of belly that is protruded to the point $(c,0)$, with the body being to the right. If $c=0$, then $(0,0)$ is a singularity that is called *cusp*. Assume $c\neq 0$. Then in each case there are two inflexion points. If $c<0$, then the curve passes through stationary inflexion points $(0,\pm c^{3/2})$. If $c>0$, then the inflexion points are at $(2^{2/3}c,\pm 3^{1/2}c^{3/2})\approx(1.6c,1.7c^{3/2})$ and the slope of the inflexion line is equal to $2^{1/3}(3c)^{1/2}\approx 2.2c^{3/2}$.

If $x_2^2=x_1^3-c^2x_1$, then it may be assumed that $c>0$ since $x^3-c^2x=x(x-c)(x+c)$. In this case the curve has two affine branches. One has a form of an oval with the flat pole at $(-c,0)$, with the other pole at $(0,0)$ and with extreme points at $(-3^{-1/2}c,\pm 2^{1/2}\cdot 3^{-3/4}c^{3/2})\approx(-0.58c,0.62c^{3/2})$. The central part has again a belly-like form with the body right of $(c,0)$. The inflexion points are at $\approx(1.5c,1.3c^{3/2})$ and the slope of inflexion line is $\approx 2.1c^{1/2}$.

The shape of the unbounded branch in the above two examples does not seem to resemble a cut of a torus. However, the resemblence is topological, up to deformation. From the projective point of view the branch passes through the point at infinity, and that makes it closed.

To finish the classification of shapes of real Weierstrass curves consider the curve given by $x_2^2=x_1(x_1-1)^2=x_1^3-2x_1^2+x_1$. The curve passes through points $(4,6)$, $(1,0)$, $(1/3,-4/\sqrt{27})\approx(0.33,-0.77)$, $(0,0)$, $(1/3,4/\sqrt{27})$, $(1,0)$, $(4,-6)$, forming thus a crossing point at $(1,0)$. This type of singularity is called a *node*.

W.3. **The group of an elliptic curve.** The K-rational points of a projective smooth Weierstraß curve may be equipped with a group structure. This is well known and will be considered in detail later. The aim here is to give a certain idea what is the abstract background of such groups. It turns out that they may be defined only in terms of the function field $K(C)$, where C is an elliptic curve (thus each elliptic curve induces a group structure, not only smooth Weierstraß curves).

In this context the following metaphor may be of help. The genus of a surface measures, in some sense, what is missing. If $A\leq B$ are abelian groups, then what is missing to A may be expressed by factorization B/A.

Situations when B and A are infinite, but the factor may be finite and nontrivial, tend to be mathematically interesting. In our case B is a subgroup of free abelian group with the basis being equal to the set of all places of $K(C)$. Elements of that group are formal sums $\sum a_P P$, where P runs through all places and $a_P\in\mathbb{Z}$ is nonzero for only finitely many P. Elements with $\sum a_P\deg(P)=0$ form the subgroup B, while the group A coincides with the set of all principal divisors. If Q is a fixed place of degree one, then it may be proved that each element of B/A (i.e., each coset modulo A) contains a unique element of B that is equal to $P-Q$, where P is a place of degree one.

If the curve C is smooth at each K-rational point, then each such P may be associated with a single K-rational point. Denote P by P_α if P is associated with a K-rational point α. Thus $Q=P_\omega$ for a K-rational point ω.

Facts above imply that adding the coset of $P_\alpha-P_\omega$ with the coset of $P_\beta-P_\omega$ yields a coset with some $P_\gamma-P_\omega$. Setting $\gamma=\alpha\oplus\beta$ equips the K-rational points of C with the structure of an abelian group, and ω is the neutral element of this group.

Formulae for computing $\oplus$ depend upon the definition of C. It occurs quite often that a choice has to be made between several formulae. The choice depends upon values of α and β, and upon their relationshiop. A situations when there exists a universal formula (called also a *closed* formula) which works for all α and β is of certain computational advantage.

W.4. **Applications of elliptic curves.** Some applications are standard and some are emerging. The *Elliptic curve cryptography* (ECC) usually refers to the bunch of applications that replace counting modulo a prime by computations in a subgroup of the group of an elliptic curve. If C is an elliptic curve over K, then $C(K)$ refers to the group operation $\oplus$ that is defined upon the K-rational points of C. The neutral element ω of the group is usually understood from the context. In applications K is a finite field. Thus $K = \mathbb{F}_q$, where q is a power of a prime. In present applications q is nearly always a large prime. Structure of $\mathbb{F}_q$ implies that for large q the group $C(\mathbb{F}_q)$ always contains a large cyclic subgroup. The order of this subgroup appears to be a random feature (while it has to occur in a certain interval). There are thus many situations when $C(\mathbb{F}_q)$ contains a large cyclic subgroup G that is of prime order. A generator of this subgroup, often denoted by P, usually constitutes, together with parameters of the curve C, the public key (or a part of it).

Note that making public the pair (P, C) does not imply knowledge of $|G|$ or $|C(K)|$. Classical protocols (Diffie-Hellman, Elgamal etc.) derive their security from the difficulty of the Discrete Logarithm Problem (DLP). Some of the attacks on the DLP require knowledge of the order of the group. The order of $C(K)$ is given by the number of K-rational points. There does not seem to exist any straightforward way how to determine this number from the parameters of the curve. In the context of ECC the point counting algorithms are thus of paramount importance.

The advantage of ECC over modular arithmetic rests in the fact that the DLP is more difficult, which allows for shorter keys. However, quantum computing makes all protocols based upon the DLP vulnerable. One of the promising alternatives for elliptic postquantum cryptography is based on isogenies of supersingular elliptic curves. That is presently beyond the scope of this text.

Classical applications of ECC need keys of considerable size (while much shorter than those needed for RSA). The speed of computation is hence a factor to be considered. The question is not only how to compute $\alpha \oplus \beta$, but also how to organize a computation of $[n]\alpha = \alpha \oplus \cdots \oplus \alpha$. In general, techniques used do not differ from those for other cyclic groups. In some cases (like Elliptic Curves Digital Signature Algorithm, the ECDSA) only the x-coordinate α of the point (α, β) is used. There are some speed-ups that take advantage of this fact.

Elliptic curves are also used for pseudorandom generators and in factorizing integers. Integers that are accessible by Lenstra elliptic-curve factorization are smaller than those accessible by the Number Field Sieve (NFS). However, the NFS uses many auxiliary factorizations of small integers, and for that the elliptic-curve factorization appears to be the most efficient.