A Quick Introduction to Algebraic Geometry and Elliptic Curves [1]

D.S. Nagaraj and B. Sury

In this volume, there are articles on the following topics in elliptic curves: Mordell-Weil theorem, Nagell-Lutz theorem, Thue's theorem, Siegel's theorem, ℓ-adic representation attached to an elliptic curve over a number field, Weil conjectures for elliptic curves over finite fields, p-adic theta functions and Tate curves and Complex Multiplication. In these articles, the basic theory of elliptic curves is assumed. As an introduction to the basics, there are now many good texts available. The standard texts are Silverman's book [S] and Cassels's book [C]. However, for the sake of self-containment and easy reference, we present here a very brief review of the basic background and theory by assuming some basic knowledge of field theory. We shall start with the basic definitions in algebraic geometry for which one could consult any standard text (for instance, [M]). Some proofs of results on elliptic curves have been sketched here. We have benefitted from a set of unpublished lecture notes of an Instructional conference on elliptic curves held at the Tata Institute of Fundamental Research, Mumbai in 1991. For more details one may consult [S].

1. Affine and Projective Varieties

Let K be a field and $\bar{K}$ be a fixed algebraic closure. The set

$$\mathbb{A}^n_K = \{\underline{x} = (x_1, \ldots, x_n) | x_i \in \bar{K} \ (1 \leq i \leq n)\}$$

is called the *affine* n-space over a field K. For each field $L \supseteq K$ the set

$$\mathbb{A}^n(L) = \{\underline{x} = (x_1, \ldots, x_n) \in \mathbb{A}^n_L \,|\, x_i \in L \ (1 \leq i \leq n)\}$$

is called the L-valued points of the affine n-space. Note that if $L \supseteq K$ is an algebraically closed field then $\mathbb{A}^n_L = \mathbb{A}^n(L)$.

[1] Elliptic Curves, Modular Forms and Cryptography, *Proceedings of the Advanced Instructional Workshop on Algebraic Number Theory, HRI, Allahabad, 2000* (Eds. A. K. Bhandari, D. S. Nagaraj, B. Ramakrishnan, T. N. Venkataramana), Hindustan Book Agency, New Delhi 2003, pp. 5–31.

2000 *Mathematics subject classification.* Primary: 14H05, 14H52, 14K05.

For a field L the polynomial ring $L[X_1, \ldots, X_n]$ in n variables over L is denoted by $A_{n,L}$. For $f_1, \ldots, f_r \in A_{n,\bar{K}}$ the subset $V(f_1, \ldots, f_r)$ of $\mathbb{A}^n_K$ defined by

$$V(f_1, \ldots, f_r) = \{\underline{x} \in \mathbb{A}^n_K \mid f_1(\underline{x}) = \cdots = f_r(\underline{x}) = 0\}$$

is called an *Affine algebraic set*.

We get a topology on $\mathbb{A}^n_K$ called the *Zariski topology* for which the closed sets are precisely affine algebraic sets in $\mathbb{A}^n_K$. Thus open sets for the Zariski topology are of the form $\mathbb{A}^n_K - V$, where V is an affine algebraic set. Open sets of the form $D(f) = \mathbb{A}^n_K - V(f)$, $f \in A_{n,\bar{K}}$ form a basis for the Zariski topology and they are known as *basic open sets*.

For any subset A of $\mathbb{A}^n_K$, the Zariski topology induces a topology on A which is called the Zariski topology on A.

The product of the affine n space $\mathbb{A}^n_K$ with the affine m space $\mathbb{A}^m_K$ is defined as the affine $n+m$ space $\mathbb{A}^{n+m}_K$. More generally, the product of algebraic sets $V_1 \subset \mathbb{A}^n_K$ and $V_2 \subset \mathbb{A}^m_K$ is the set $V_1 \times V_2 \subset \mathbb{A}^n_K \times \mathbb{A}^m_K$ with induced Zariski topology. Thus, with the above definition the product of algebraic sets is an algebraic set.

The Zariski topology on $\mathbb{A}^{n+m}_K$ is not the product topology. For example, as a set $\mathbb{A}^2_K$ is $\bar{K} \times \bar{K}$ but the Zariski topology on $\mathbb{A}^2_K$ is not the product topology; in fact there are more Zariski-open sets in $\mathbb{A}^2_K$ than there are in the product topology. For instance, the set $\{(x, y) \in \bar{K}^2 : xy \neq 1\}$ is open in the Zariski topology but not in the product topology.

Given an affine algebraic set $V \subseteq \mathbb{A}^n_K$, the set

$$I(V) = \{f \in A_{n,\bar{K}} | f(\underline{x}) = 0, \ \forall \underline{x} \in V\}$$

is an ideal in the ring $A_{n,\bar{K}}$. If the ideal $I(V)$ is generated by $g_1, \ldots, g_k \in A_{n,K}$ then V is said to be *defined over* K.

If the affine algebraic set $V \subseteq \mathbb{A}^n_K$ is defined over K by $f_1, \ldots, f_r \in A_{n,K}$, then for any field L such that $K \subseteq L$ the set

$$V(L) = \{\underline{x} \in \mathbb{A}^n(L) \,|\, f_1(\underline{x}) = \cdots = f_r(\underline{x}) = 0\}$$

is called the L-valued points of the affine algebraic set V.

An affine algebraic set V is said to be an *affine variety* or a *variety* if the ideal $I(V)$ is a prime ideal. If an affine variety V is defined over K then

it is called a K–affine variety or K–*variety*. If V and W are K-varieties and $W \subset V$ then the open set $V - W$ of V is called a K-open set.

1) Let $\mathbb{Q}$ denote the field of rational numbers, let $L = \mathbb{Q}(\sqrt{2})$, and $f = x - \sqrt{2}$. Then, the variety V defined by f is defined over L but not defined over $\mathbb{Q}$.
2) Let $\mathbb{R}$ denote the field of real numbers. The affine variety V defined by the polynomial $X^2 + Y^2 + 1$ is a $\mathbb{R}$–variety. Note that $V(\mathbb{R}) = \emptyset$.

If V is an affine variety then the ring

$$A(V) = \frac{A_{n,\bar{K}}}{I(V)}$$

is called the *coordinate ring* of V and elements of $A(V)$ are called *regular functions* on V. Note that regular functions are continuous functions from $V \to \mathbb{A}^1$ for the Zariski topology.

If V is a K–variety then

$$A_K(V) = \frac{A_{n,K}}{I(V) \cap A_{n,K}}$$

is called the K–coordinate ring of the K–variety V and $A_K(V)$ is a subring of $A(V)$ in a natural way.

Let V be an algebraic set. Note that every $f \in A(V)$ is a restriction of a polynomial function $\bar{K}^n \to \bar{K}$ and two polynomial functions $f, g : \bar{K}^n \to \bar{K}$ defines the same regular function on V if and only if $f - g \in I(V)$.

For a variety (respectively, K–variety) V the quotient field $\bar{K}(V)$ (respectively, $K(V)$) of the coordinate ring $A(V)$ (respectively, K– coordinate ring $A_K(V)$) is called *field of rational functions* (respectively, *field of K–rational functions*) on V. The elements of $\bar{K}(V)$ (respectively, $K(V)$) are called rational functions (respectively, K–rational functions) on V. Every rational function (K–rational function) on V is a regular function on an open set (K–open set).

If V and W are two affine varieties over K then a map $\phi : V \to W$ is said to be a *morphism* of varieties if and only if $f \circ \phi \in A(V)$ for every $f \in A(W)$. A morphism $\phi : V \to W$ of varieties induces an homomorphism $\phi^* : A(W) \to A(V)$ of coordinate rings. Note that a morphism of varieties is continuous for the Zariski topology.

For a variety V we denote by Id_V the identity morphism of V.

If V and W are K–varieties and if the morphism ϕ is such that the homomorphism ϕ^* induces a homomorphism $A_K(W) \to A_K(V)$ then ϕ is said to be a K–morphism. Note that if V is a K–variety then Id_V is K–morphism.

A morphism (respectively, K–morphism) $\phi : V \to W$ of varieties (respectively, K–varieties) is said to be an *isomorphism* if there exists a morphism (respectively, K–morphism) $\psi : W \to V$ of varieties (respectively, K–varieties) such that $\psi \circ \phi = \mathrm{Id}_V$ and $\phi \circ \psi = \mathrm{Id}_W$. An isomorphism (respectively, K-isomorphism) $\phi : V \to V$ is called an *automorphism* (respectively, K-automorphism).

A morphism (respectively, K–morphism) $\phi : V \to W$ of varieties over $\bar{K}$ (respectively, K–varieties) is said to be *dominant* if $\phi^* : A(W) \to A(V)$ (respectively, $\phi^* : A_K(W) \to A_K(V)$) is an injective homomorphism.

For example, consider $V = \{(x, y) \in \mathbb{A}^2_{\bar{K}} : xy = 1\}, W = \mathbb{A}^1_{\bar{K}}$. Then, the first projection $V \to W; (x, y) \mapsto x$ is a dominant morphism. Note that it is not surjective.

A morphism (respectively, K–morphism) $\phi : V \to W$ of varieties over $\bar{K}$ (respectively, K–varieties) is said to be *finite* if $\phi^* : A(W) \to A(V)$ (respectively, $\phi^* : A_K(W) \to A_K(V)$) is an integral extension (i.e., every element $f \in A(V)$ (respectively $f \in A_K(V)$) satisfies a polynomial equation $f^n + a_1 f^{n-1} + \cdots + a_n = 0$ for some $n \geq 1$ with $a_i \in \phi^* A(W)$ (respectively, $a_i \in \phi^* A_K(W)$), for each $i (1 \leq i \leq n)$.

Let $\phi : V \to W$ be a dominant morphism of varieties over $\bar{K}$. Then the homomorphism of $\phi^* : A(W) \to A(V)$ induces an inclusion of fields $\phi^* : \bar{K}(W) \to \bar{K}(V)$. If this field extension is separable (respectively, purely inseparable) we say that the morphism ϕ is *separable* (respectively, *purely inseparable*)

Examples :
(i) Let K be a field of characteristic $p \neq 0$. Let $V = \mathbb{A}^1_K = W, \phi : V \to W; x \mapsto x^p$ (the Frobenius morphism). Then, ϕ is purely inseparable.
(ii) In the above example, $\psi = Id - \phi : x \mapsto x - x^p$ is separable.
(iii) The morphism $\psi \circ \phi$ is inseparable but not purely inseparable.

A K-algebra A is said to be *finitely generated* K-algebra if it is a quotient of a polynomial ring in finitely many variables over K. Note that the K- affine coordinate ring of a K-affine variety is an example of a finitely generated K-algebra. For a finitely generated K-algebras one has the following result:

Nöether Normalization Lemma: *Let A be a finitely generated K-algebra. Assume A is an integral domain. Then there exists $f_1, \ldots, f_n \in A$ such that the subalgebra $K[f_1, \ldots, f_n]$ generated by $f_1, \ldots, f_n$ over K is isomorphic to the polynomial algebra $K[X_1, \ldots X_n]$ and A is an integral extension over $K[f_1, \ldots, f_n]$. The integer n depends only on A.*

Let $A_K(V)$ be the K coordinate ring of a affine K variety V. The integer n of the Nöether Normalization lemma is called the *dimension* of the affine K-variety V. Note that the dimension of the variety V is also the transcendental degree over K of the quotient field $K(V)$ of $A_K(V)$.

For instance, $\mathbb{A}^n_K$ has dimension n. $V = \{(x, y) \in \mathbb{A}^2_K : x^n + y^n = 1\}$ is an affine variety of dimension one. An affine variety V of dimension one is called an affine curve. An affine variety V of dimension two is called an affine surface.

Let $V \subset \mathbb{A}^n$ be an affine variety over K of dimension m. A point $p \in V$ is said to be a *non-singular point* of V if there exist $g_1, \ldots, g_{n-m} \in I(V)$ and an open subset $U \subset \mathbb{A}^n$ such that $V \cap U = V(g_1, \ldots, g_{n-m}) \cap U$ and the $(n - m) \times n$ matrix

$$(\partial g_i / \partial x_j)_{1 \leq i \leq n-m, 1 \leq j \leq n}$$

has rank $n - m$ at every point of $V \cap U$. A variety V is *non-singular* if every point of V is a non-singular point. Some examples appear in § 2.

If $\phi : V \to W$ is an isomorphism of varieties then it can be shown that a point $p \in V$ is non-singular if, and only if, the point $\phi(p) \in W$ is non-singular. Thus, the property of non-singularity is independent of the embedding.

The *projective* n-space $\mathbb{P}^n_K$, over K, is the set of all lines through the origin in the $n + 1$ dimensional vector space $\bar{K}^{n+1}$ over $\bar{K}$. Thus

$$\mathbb{P}^n_K = \frac{\bar{K}^{n+1} - \{(0, \ldots, 0)\}}{\sim}$$

where $\sim$ is the equivalence relation defined by $\underline{x} \sim \underline{y}$ if and only if $\underline{x} = \lambda \underline{y}$ for some $\lambda \in \bar{K} - (0)$.

For each field $L \supseteq K$ the subset

$$\mathbb{P}^n(L) = \{\underline{x} = [(x_1, \ldots, x_{n+1})] \in \mathbb{P}^n_L | x_i \in L \ (1 \leq i \leq n + 1)\}$$

is called the L-valued points of the projective n-space over L. Note that if L is an algebraically closed field then $\mathbb{P}^n_L = \mathbb{P}^n(L)$.

For a field L we denote by $A^h_{n+1,L}$ the set of homogeneous polynomials in $A_{n+1,L}$. If $f \in A^h_{n+1,\bar{K}}$ and $\underline{x} \in \bar{K}^{n+1} - (0,\ldots,0)$ then $f(\underline{x})$ is zero if and only if $f(\lambda\underline{x})$ is zero for every $\lambda \in \bar{K} - (0)$. Hence for $\underline{x} \in \mathbb{P}^n_K$ it makes sense to talk about $f(\underline{x})$ being zero or not. For $f_1,\ldots,f_r \in A^h_{n+1,\bar{K}}$ the subset $Z(f_1,\ldots,f_r)$ of $\mathbb{P}^n_K$ defined by

$$Z(f_1,\ldots,f_r) = \{\underline{x} \in \mathbb{P}^n_K \mid f_1(\underline{x}) = \cdots = f_r(\underline{x}) = 0\}$$

is called a *Projective algebraic set.*

We get a topology on $\mathbb{P}^n_K$ called the *Zariski topology* for which the closed subsets are precisely projective algebraic sets. If $A \subset \mathbb{P}^n_K$ then we get an induced topology on A which is also called the Zariski topology on A. For any $i\,(1 \le i \le n+1)$ the open set

$$U_i = \{[(x_1,\ldots,x_{n+1})] \in \mathbb{P}^n_K \,|\, x_i \neq 0\}$$

of $\mathbb{P}^n_K$ can be identified with $\mathbb{A}^n_K$ by the map which sends $[(x_1,\ldots,x_{n+1})] \in U_i$ to $(\frac{x_1}{x_i},\ldots,\frac{x_{i-1}}{x_i},\frac{x_{i+1}}{x_i},\ldots,\frac{x_n}{x_i}) \in \mathbb{A}^n_K$. Under this identification the Zariski topology on U_i and the Zariski topology on $\mathbb{A}^n_K$ coincides. Thus we see that any projective algebraic set is a finite union of affine algebraic sets which are open.

The set theoretic map $\phi : \mathbb{P}^n_K \times \mathbb{P}^m_K \to \mathbb{P}^{(n+1)(m+1)-1}_K$ defined by $([(x_1,\ldots,x_{n+1})],[(y_1,\ldots,y_{m+1})]) \mapsto [(x_1y_1,\ldots,x_1y_{m+1},x_2y_1,\ldots,x_{n+1}y_{m+1})]$ is bijective onto the projective subvariety defined by the vanishing of the 2×2 minors of the $(n+1)\times(m+1)$ matrix

$$(Z_{ij})_{1\le i\le n+1, 1\le j\le m+1}\,,$$

where $Z_{ij}, (1 \le i \le n+1, 1 \le j \le m+1)$ are homogeneous functions of the homogeneous coordinate system $[(z_{11},\ldots,z_{1(m+1)},z_{21},\ldots,z_{(n+1)(m+1)})]$ on $\mathbb{P}^{(n+1)(m+1)-1}_K$. With the above identification we get projective variety structure $\mathbb{P}^n_K \times \mathbb{P}^m_K$. This projective variety is called the product of projective spaces $\mathbb{P}^n_K$ and $\mathbb{P}^m_K$. Using the above definition one gets product of projective algebraic sets as a projective algebraic set.

A projective algebraic set Z in $\mathbb{P}^n_K$ is said to be a *Projective variety* (respectively, *Projective K–variety*) if for each $i\,(1 \le i \le n+1)$ the affine algebraic set $Z \cap U_i$ is a variety (respectively, K–variety).

It is easy to see that product of projective varieties is again a projective variety.

Let Z and W be two projective varieties over K. A map $\phi : Z \to W$ is said to be a morphism of projective varieties if the following holds: for each point $z \in Z$ there exist open sets $U_z \subset Z$, $V_{\phi(z)} \subset W$ such that $z \in U_z,\ \phi(z) \in V_{\phi(z)}$ are affine varieties, $\phi(U_z) \subset V_{\phi(z)}$ and $\phi|_{U_z} : U_z \to V_{\phi(z)}$ is a morphism of affine varieties.

As in the case of affine varieties we can define isomorphism and automorphism for projective varieties. Moreover, K–morphisms, K–isomorphisms and K–automorphisms of projective K-varieties are defined in a similar fashion.

Consider F/G, with $F, G \in A^h_{n+1,\bar{K}}$ of same degree and $G \not\equiv 0$ on V; let us call two such elements F/G and F_1/G_1 to be equivalent if $FG_1 - F_1G \equiv 0$ on V. For any V, the equivalence classes form a field which we denote by $\bar{K}(V)$. Similarly, $K(V)$ can be defined for a K-variety V. For a projective variety (respectively, projective K–variety) $V \subset \mathbb{P}^n$ we denote by V_i $(1 \leq i \leq n+1)$ the open set $V \cap U_i$ $(1 \leq i \leq n+1)$. As we have remarked earlier, V_i are affine open subvarieties of V. Then, the quotient fields $\bar{K}(V_i)$ (respectively, $K(V_i)$) are all isomorphic to the field $\bar{K}(V)$ (respectively, $K(V)$). We call any one of them *field of rational functions* (respectively, *field of K-rational functions*) on V and is denoted by $\bar{K}(V)$ (respectively, $K(V)$). The elements of $\bar{K}(V)$ (respectively, $K(V)$) are called *rational functions* (respectively, *K–rational functions*) on V. Every rational function (K–rational function) on V is a regular function on an affine open set (affine K–open set) of V. Given a point p on V, the *local ring $\mathcal{O}_p$ at p* is defined to be the subring. Similarly, one can define the local ring at a K-point of a K-variety; it will be a subring of $\bar{K}(V)$ consisting of all $f \in \bar{K}(V)$ which are regular in an affine open subset of V containing p. A rational function on V is said to be regular if it is regular on each V_i. Note that it can be shown without too much difficulty that, on a projective variety, the only regular functions are the constant functions. This is analogous to the fact that there are no holomorphic non constant functions on a compact complex manifold. For a projective variety V over K, the transcendental degree of $\bar{K}(V)$ over $\bar{K}$ is called the *dimension* of V.

A projective variety of dimension one is called a projective curve. Some examples of projective curves are given in § 2. A projective variety of dimension two is called a projective surface.

A morphism (respectively, K–morphism) $\phi : V \to W$ of projective varieties over $\bar{K}$ (respectively, K–varieties) such that $\phi(V) = W$ induces an injective homomorphism $\phi^* : \bar{K}(W) \to \bar{K}(V)$ (respectively, $\phi^* : K(W) \to K(V)$). If $\bar{K}(V)$ (respectively, $K(V)$) is separably generated field over $\phi^*(\bar{K}(W))$ (respectively, $\phi^*(K(W))$) then ϕ is said to be separable. Similarly we can define purely inseparable morphisms.

Let C_1 and C_2 be two curves over an algebraically closed field K. Then it can be shown that giving a non constant morphism $\phi : C_1 \to C_2$ of projective varieties over K is equivalent to giving an injective homomorphism $\phi^* : K(C_2) \to K(C_1)$ of fields which is identity on K.

The following is a useful fact on fibres (See [S], Proposition 2.6):

Lemma *If $f : X \to Y$ is a non constant morphism between nonsingular algebraic curves over $\bar{K}$, then, for all but a finite number of points y of Y, the fibre $f^{-1}(y)$ consists precisely of $[K(X) : f^*K(Y)]_{sep}$ points.*

Here $[L : K]_{sep}$ denotes the separability degree of a field extension L over K. The integer $[K(X) : f^*K(Y)]_{sep}$ is called the *separability degree* of f. It is denoted $\deg_{sep}(f)$ and equals $\deg(f) := [K(X) : f^*K(Y)]$ if f is a separable morphism. The integer $\deg(f)/(\deg_{sep}(f))$ is called the inseparable degree of f and is denoted by $\deg_{insep}(f)$.

A point p of a projective variety V is said to be *non-singular* if p is a non-singular point of an affine open subset U of V. If every point p of V is non-singular then we say that V is a non-singular projective variety. The following is an important property of projective varieties.

Rigidity of projective varieties: *Let X, Y be projective varieties and, $\theta : X \times X \to Y$ a morphism such that $\theta(X \times \{x_0\}) = \{y_0\}$. Then, there exists a morphism $\phi : X \to Y$ such that $\theta = \phi \circ \pi_2$, where $\pi_2 : X \times X \to X$ is the second projection.*

2. Plane curves

Let K be any field and let f be a non constant polynomial in two variables X, Y with coefficients from K. If f is irreducible over the algebraic closure $\bar{K}$ of K, it defines an *affine plane curve* C_f over K; for each field $L \supseteq K$, the L-points of C_f is the set $C_f(L) = \{(x, y) \in \mathbb{A}^2(L) : f(x, y) = 0\}$. Note that a point $p \in C_f(L)$ is *nonsingular* if, not both $\frac{\partial f}{\partial x}$ and $\frac{\partial f}{\partial y}$ are zero at p. C_f is said to be nonsingular if all points in $C_f(\bar{K})$ are nonsingular.

For instance, the curve C_f given by $f(X,Y) = Y^2 - X^3 - aX - b$ over a field K with char $K \neq 2$, is nonsingular if, and only if, the *discriminant* of $4a^3 + 27b^2$ is non-zero. This discriminant is denoted by $\Delta(f)$.

Let F be a homogeneous polynomial in three variables over K which has no multiple irreducible factors over $\bar{K}$. Then, $C_F \subset \mathbb{P}^2_K$ defined by F is called a *projective plane curve* over K. For any $L \supseteq K$, the L-points of C_F are defined as $C_F(L) = \{[(x,y,z)] \in \mathbb{P}^2(L) : F(x,y,z) = 0\}$. The degree of the homogeneous polynomial F is called the *degree* of the curve C_F in $\mathbb{P}^2_K$.
If C_F, C_G are two projective plane curves over K where F, G do not have any irreducible common factor over $\bar{K}$, then $C_F(\bar{K})$ and $C_G(\bar{K})$ intersect in ($\deg F$)($\deg G$) points when counted with multiplicity. This is known as *Bezout's theorem.*

The projective plane curve C_F with $F(X,Y,Z) = Y^2Z - X^3 - aXZ^2 - bZ^3$ meets the *line at infinity* $Z = 0$ in $\mathbb{P}^2$ at the point $[(0,1,0)]$ of $\mathbb{P}^2_K$.

A curve of degree 1 in $\mathbb{P}^2_K$ is a line $C : aX + bY + cZ = 0$ with not all a, b, c zero. Such a curve always has L-points for any $L \supseteq K$. In fact, if $a \neq 0$, the L-points can be parametrized by $\mathbb{P}^1(L)$ viz., the morphism sending $[(y,z)] \in \mathbb{P}^1(L)$ to $[(\frac{-by-cz}{a}, y, z)] \in C(L)$ is an isomorphism.

A projective plane curve given by a degree 2 polynomial in three variables over K is known as a conic; it may not have any L-points for a given field $L \supseteq K$. If C is a conic which does have an L-point p, then all the points of $C(L)$ can be parametrized by a $P^1(L)$ (viz., the lines in $P^2(L)$ passing through p). For instance, if C is defined by $X^2 + Y^2 - Z^2 = 0$, then taking p to be the point $(-1,0,1)$, the points of $C(L)$ are $[(x^2 - y^2, 2xy, x^2 + y^2)]$, with $[(x,y)] \in \mathbb{P}^1(L)$.

Let $\mathbb{Q}$ be the field of rational numbers. In number theory, one often considers curves C over $\mathbb{Q}$ and looks for K-points for an algebraic number field K. If C has degree 2, there is a local-global principle showing that existence of K-points is a question that reduces to the question over the various completions.

In the case of the curve $C : X^2 + Y^2 = Z^2$, we parametrized the points and this parameterizes the affine curve $X^2 + Y^2 = 1$ (over $\mathbb{Q}$ or $\mathbb{R}$, say, where $\mathbb{R}$ is the field of real numbers,) by the non constant rational functions $\frac{t^2-1}{t^2+1}, \frac{2t}{t^2+1}$ in a parameter t. On the other hand, the Fermat curve $x^n + y^n = 1$ for $n \geq 3$ cannot be parametrized rationally over a field K if the characteristic of K does not divide n. In other

words, the analogue of Fermat's last theorem is valid over $K(t)$ for such K and n. This is seen as follows.

Lemma (*abc* conjecture for the ring $K[t]$)
Let K be any field and suppose $a(t), b(t), c(t) \in K[t]$ are pairwise coprime polynomials such that $a(t) + b(t) = c(t)$ and at least one of them is non constant. If at least one of $a(t), b(t), c(t)$ is separable, then

$$Max(\deg a(t), \deg b(t), \deg c(t)) \leq N - 1,$$

where N is the number of distinct roots of $a(t)b(t)c(t)$.

Proof: Note that the coprimality assumption already implies that none of the polynomials $a(t), b(t), c(t)$ is the zero polynomial. To see this, we may assume that K is algebraically closed and, let us write

$$a(t) = c_1 \prod_1^k (t - \alpha_i)$$

$$b(t) = c_2 \prod_1^l (t - \beta_i)$$

$$c(t) = c_3 \prod_1^m (t - \gamma_i),$$

where $c_i \in K$ and the roots may be repeated. We may assume that c is separable without loss of generality. Recall that for any polynomial $u(t) = \sum_{i=0}^r u_i t^i \in K[t]$, one defines the polynomial $u'(t) := \sum_{i=1}^r i u_i t^{i-1}$. For rational functions $f(t) = \frac{u(t)}{v(t)} \in K(t)$, one defines $f'(t) = \frac{u(t)'v(t) - u(t)v'(t)}{v(t)^2}$. One calls a non constant polynomial u separable if u' is not the zero polynomial. It is easy to see that $(f+g)' = f' + g'$ and $(fg)' = f'g + fg'$ in $K(t)$. Hence, if $u(t) = c\prod_{i=1}^r (t - u_i)$ with $c \in K$, then $u'(t) = c\sum_{i=1}^r \prod_{j \neq i} (t - v_j)$. Therefore, in our equation, if we put $f(t) = \frac{a(t)}{c(t)}$ and $g(t) = \frac{b(t)}{c(t)}$, then $f(t) + g(t) = 1$ and so, $f' + g' = 0$ in $K(t)$. Note that if $g' = 0$, then $\frac{b'c - bc'}{c^2} \neq 0$ i.e., $bc' = b'c$. Since b, c are coprime polynomials, c will have to divide c' which is not the zero polynomial (as c is separable) and has smaller degree. This contradiction implies that $g' \neq 0$. Now, a simple computation gives

$$\frac{b(t)}{a(t)} = \frac{g}{f} = -\frac{f'/f}{g'/g} = \frac{c'/c - a'/a}{b'/b - c'/c} = \frac{-\sum_1^k \frac{1}{t-\alpha_i} + \sum_1^m \frac{1}{t-\gamma_i}}{\sum_1^l \frac{1}{t-\beta_i} - \sum_1^m \frac{1}{t-\gamma_i}}.$$

Call the numerator and the denominator of the right side as $B(t)$ and $A(t)$. Both $A(t)$ and $B(t)$ can be made into polynomials by multiplying by a common polynomial $R(t)$ of degree N, where N is the number of distinct roots of $a(t)b(t)c(t)$. We have $\frac{b(t)}{a(t)} = \frac{R(t)B(t)}{R(t)A(t)}$ which gives $b(t)R(t)A(t) = a(t)R(t)B(t)$. Since $a(t), b(t)$ are coprime, their degrees are at the most those of $R(t)A(t)$ and $R(t)B(t)$ respectively. The latter degrees are at the most $N-1$. Thus, $\mathrm{Max}(\deg a(t), \deg b(t), \deg c(t)) \leq N-1$, where N is the number of distinct roots of $a(t)b(t)c(t)$. This proves the lemma.

This lemma can be used to prove that the Fermat equation does not have any non constant solutions in $K[t]$ if $n \geq 3$ and is relatively prime to the characteristic of K. But, we give below a simpler proof for this. We prove :

Lemma *Consider the generalized Fermat curve $aX^n + bY^n = 1$, where $a, b \in K^*$. Assume that $n \geq 3$ if characteristic of K is 0 and if the characteristic of K is $p > 0$, then $n = p^d n_0$ where $(p, n_0) = 1$ and $n_0 \geq 3$. Then, this curve is not rational.*

Proof: By replacing K by its algebraic closure, we may assume that K is algebraically closed. Suppose the curve is rational. Then, $X(t) = \frac{p(t)}{r(t)}, Y(t) = \frac{q(t)}{r(t)}$ where $p(t), q(t), r(t)$ are pairwise coprime polynomials in $K[t]$ satisfying $aX(t)^n + bY(t)^n = 1$. If char $K = p > 0$, we observe first that we may assume that $n \geq 3$ is coprime to p. The reason is as follows. By assumption, if char $K = p > 0$, then $n = p^d n_0$ with $(p, n_0) = 1$ and $n_0 \geq 3$; thus a nontrivial solution to the equation $aX(t)^n + bY(t)^n = 1$ gives one for the equation $a_1 X(t)^{n_0} + b_1 Y(t)^{n_0} = 1$ where $a_1^{p^d} = a, b_1^{p^d} = b$. Thus, we may work with $n_0 \geq 3$ which is coprime to p. So, $ap(t)^n + bq(t)^n = r(t)^n$. Since char K does not divide n, we get $ap(t)^{n-1}p'(t) + bq(t)^{n-1}q'(t) = r(t)^{n-1}r'(t)$. Thus, one can think of these as a system of two linear equations for $ap(t)^{n-1}, bq(t)^{n-1}, r(t)^{n-1}$ in $K[t]$. Eliminating $p(t)^{n-1}$, one has

$$q(t)^{n-1}(p'(t)q(t) - p(t)q'(t)) = r(t)^{n-1}(r(t)p'(t) - p(t)r'(t)).$$

Eliminating $q(t)^{n-1}$, one has

$$p(t)^{n-1}(p'(t)q(t) - p(t)q'(t)) = r(t)^{n-1}(q(t)r'(t) - r(t)q'(t)).$$

As $p(t), q(t), r(t)$ are coprime, one gets $q(t)^{n-1}$ divides $r(t)p'(t) - p(t)r'(t)$ and $p(t)^{n-1}$ divides $q(t)r'(t) - r(t)q'(t)$. Similarly, we get $r(t)^{n-1}$ divides $q(t)p'(t) - p(t)q'(t)$. Let us write $k \geq l \geq m$ for the degrees of

$p(t), q(t), r(t)$ respectively. Note that $q(t)r'(t) - r(t)q'(t)$ cannot be the zero polynomial unless $q(t), r(t)$ are constants. In such a case, $p(t)$ is also constant, which contradicts the assumption that one has a rational parametrisation. Therefore, $q(t)r'(t) - r(t)q'(t)$ is not the zero polynomial and the fact that $p(t)^{n-1}$ divides it implies $(n-1)k \leq l+m-1 \leq 2k-1$ on comparing degrees. Thus, $(n-3)a \leq -1$, a manifest contradiction of the assumption that $n \geq 3$.

Non-singular projective plane curves E over K of degree 3 will be the main topic of our discussion. Let $L \supseteq K$ be an extension field. Given two L-points of such a curve E, the chord/tangent through them meets $E(L)$ at a point of $E(L)$ again (by Bezout's theorem). This gives rise to a *group law* and later we shall see that over a number field K, the process produces all points of $E(K)$ starting from *finitely many points*. It should be noted that $E(K)$ could be empty. If $E(K)$ is non-empty, the group law is clearly commutative. Associativity is not very obvious. Here is an argument in a geometric vein. This uses the following observation:

Lemma *Let $x_1, \ldots, x_8$ be points of the plane, in 'general position' (i.e., no four lie on a line and no seven lie on a conic). Then, there is a ninth point y such that every cubic curve through $x_1, \ldots, x_8$ also passes through y.*

Proof: A cubic form $F(T) = F(T_1, T_2, T_3)$ in three variables has ten coefficients. For a point $x \in \mathbb{P}^2$ the equation $F(x) = 0$ imposes a linear condition on the coefficients of F. Therefore, making it pass through $x_1, \ldots, x_8$ imposes eight conditions (the general position hypothesis means that the eight conditions are linearly independent). So, if F_1, F_2 are two linearly independent cubic forms passing through $x_1, \ldots, x_8$, then any other cubic form passing through these eight points must be of the form $\lambda F_1 + \mu F_2$, for some λ, μ scalars. By Bezout's theorem, $F_1 = 0$ and $F_2 = 0$ have nine common points. Thus, any $\lambda F_1 + \mu F_2$ passes through these nine points.

Associativity of the group law: Let $E \subset \mathbb{P}^2$ be a non-singular cubic curve. Let O be the point of $E(K)$ which is identity for the group law. Let $a, b, c \in E(K)$. Let the lines l, m, n, r, s, t be as indicated in the figure below. That is, the line l joins a and b; it intersects $E(K)$ in the point d. The line t joins O and d and intersects $E(K)$ in the point e i.e., $a + b = e$ in $E(K)$. Let f be the third point on the intersection of $E(K)$ with the line joining c and e. Then, $(a+b)+c = e+c$ is the third point of $E(K)$ on the line Of. Similarly, $a + (b + c) = a + v$ is the third

point of $E(K)$ on Ow. We must show that both f and w are identical to the unlabeled intersection point of m and r in the figure. Consider the cubics $F_1 = lmn$ and $F_2 = rst$. Since E is a non-singular cubic passing through the eight points of intersection a, b, d, e, c, u, v, O of $F_1 = 0$ and $F_2 = 0$, the above lemma implies that it passes through the ninth point of intersection too (which is just the intersection of r and m).

r	a		w	v	
		f			
s	b	c		u	
t	d	e		O	
	l	m		n	

3. Riemann-Roch theorem and group law

Throughout this section unless mentioned otherwise, we denote by K a fixed algebraically closed field.

Let C be a non-singular, projective curve over a field K. Let $K(C)$ be the rational function field of C. We had remarked earlier that an element $f \in K(C)$ as regular function on an open set $U \subset C$. Since C is a curve, it is easy to see that f defines a morphism of varieties $f : C \to \mathbb{P}^1$. Moreover, if f is not a constant function, then the image of C under f is equal to $\mathbb{P}^1$. We think of the point $[(1, 0)] \in \mathbb{P}^1$ as the point at infinity of the open set $U_2 = \{[(x, y)] \in \mathbb{P}^1 : y \neq 0\}$ and is denoted by ∞. We identify U_2 with the affine line $\mathbb{A}^1 \simeq K$ in such a way that the point $[(0, 1)] \in U_2$ is identified with the origin $0 \in K$. If $p \in C$ is a point then the subset

$$\mathcal{O}_{C,p} = \{f \in K(C) : f(p) \neq \infty\}$$

of $K(C)$ is, in fact, a subring. This ring is a discrete valuation ring (d.v.r.) with the unique maximal ideal $m_{C,p} = \{f \in \mathcal{O}_{C,p} : f(p) = 0\}$. Thus, if we choose an element $z \in m_{C,p} - m_{C,p}^2$, then an element $h \in m_{C,p}$ can be uniquely written as $h = u.z^n$, where $n \geq 1$ is an integer and u is a unit in the ring. For $h \in m_{C,p}$, the integer n is independent of the choice of $z \in m_{C,p} - m_{C,p}^2$, we denote this integer by $ord_p(h)$. An element $h \in m_{C,p}$ such that $ord_p(h) = 1$ is called a *uniformizing*

parameter/local parameter of C at p. With the above identifications, we see that $K(\mathbb{P}^1) = K(t)$, field of rational functions in one variable t, and

$$\mathcal{O}_{\mathbb{P}^1,0} = \{f(t)/g(t) \in K(t) : f(t), g(t) \in K[t] \text{ and } g(0) \neq 0\}$$

with maximal ideal $m_{\mathbb{P}^1,0} = t\mathcal{O}_{\mathbb{P}^1,0}$. Also,

$$\mathcal{O}_{\mathbb{P}^1,\infty} = \{f(1/t)/g(1/t) \in K(t) : f(1/t), g(1/t) \in K[1/t] \text{ and } g(0) \neq 0\}$$

with maximal ideal $m_{\mathbb{P}^1,\infty} = (1/t)\mathcal{O}_{\mathbb{P}^1,\infty}$.

Let C, D be two non-singular curves over K. Let $\phi : C \to D$ be a non constant morphism. Then, we have seen that $\phi^* : K(D) \to K(C)$ is an injective homomorphism of fields. Now, if $p \in C$ is a point, it is easy to see that ϕ induces a homomorphism of rings

$$\phi_p^* : \mathcal{O}_{D,\phi(p)} \to \mathcal{O}_{C,p},$$

which takes the maximal ideal $m_{D,\phi(p)}$ into the maximal ideal $m_{C,p}$. If z is a local parameter of D at $\phi(p)$, the integer $ord_p(\phi_p^*(z))$ is independent of the local parameter z and is denoted by $e_p(\phi)$. The integer $e_p(\phi)$ is called the *ramification index* of ϕ at p. If $e_p(\phi) = 1$, then we say that ϕ is *étale* or *unramified* at p. If $e_p(\phi) > 1$, then we say that ϕ is *ramified* at p. The morphism ϕ is *étale* or *unramified* if it is so at all $p \in C$. If ϕ is a separable morphism then one can show that ϕ is unramified except for finitely many points on C. Also, it can be shown that for any point $q \in D$ the number $\sum_{p:\phi(p)=q} e_p(\phi)$ is equal to the degree of the map ϕ and hence independent of the point $q \in D$.

Let C be a non-singular curve over K and $f \in K(C)$ be a non constant rational function on C. As we have already noted, f can be thought of a morphism $f : C \to \mathbb{P}^1$. Then for a point $p \in C$ such that $f(p) = 0$ the ramification index $e_p(f)$ is called the *order of zero* of f at p. Similarly, if $p \in C$ such that $f(p) = \infty$ then $e_p(f)$ is called the *order of pole* at p.

The divisor class group of non-singular curve. Let C be a non-singular projective curve. Let $\mathrm{Div}(C)$ denote the free abelian group on $C(K)$. An element $D \in \mathrm{Div}(C)$ is of the form $D = \sum_{p \in C(K)} n_p p$, with $n_p \in \mathbb{Z}$ and $n_p = 0$ for all but finitely many $p \in C(K)$. An element of $\mathrm{Div}(C)$ is called a *divisor* on C. If $D = \sum_{p \in C(K)} n_p p$ is a divisor on C, then the integer $\sum_{p \in C(K)} n_p$ is called the *degree* of the divisor D and is denoted by $\deg(D)$. We denote by $\mathrm{Div}^0(C)$ the subgroup

of $\mathrm{Div}(C)$ degree zero divisors. An evident partial order on $\mathrm{Div}(C)$ is $D = \sum_{p \in C(K)} n_p p \geq D' = \sum_{p \in C(K)} m_p p$ if, and only if, $n_p \geq m_p$ for all $p \in C(K)$. Given a rational function f on C we associate a divisor (f) by setting $(f) = \sum_{\{p \in C(K): f(p)=0\}} e_p(f)p - \sum_{\{p \in C(K): f(p)=\infty\}} e_p(f)p$. Divisors of the form (f), $f \in K(C)$ are called *principal divisors* and by our earlier observation we see that degree of a principal divisor is zero. Since $(fg) = (f)+(g)$, the principal divisors form a subgroup of $\mathrm{Div}(C)$. Given a divisor D, there is a K vector space

$$L(D) = \{f \in K(C) : div(f) \geq -D\} \cup \{0\}.$$

We denote by $\ell(D)$ the dimension of the K-vector space $L(D)$. We have the fundamental:

Riemann-Roch Theorem: *There exists an integer g depending only on C so that for any divisor D, we have*

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

Furthermore, equality holds if $\deg D > 2g - 2$.

The number g is called the *genus* of the curve C. If C is a non-singular projective plane curve of degree d, one can show that the genus of C is $\frac{(d-1)(d-2)}{2}$ (see [S]). In particular, genus of a projective line or a non-singular conic in $\mathbb{P}^2$ is zero and that of a non-singular plane cubic is one.

Let us interpret the group law on a cubic curve using the above theorem. First, let us define the Picard group of smooth curve C. The Picard group, $\mathrm{Pic}(C)$, is the quotient group of $\mathrm{Div}(C)$ by the subgroup of of all principal divisors. Since principal divisors are of degree zero, we see that degree gives an onto homomorphism $\deg : \mathrm{Pic}(C) \to \mathbb{Z}$. The kernel of this homomorphism is denoted by $\mathrm{Pic}^0(C)$. One calls two divisors D, D' on C to be *linearly equivalent* if they define the same element of the Picard group, i.e., $D \sim D'$ if $D - D' = (f)$ for some $f \in K(C)$.

The Riemann-Roch theorem implies for a curve E of genus 1 over an algebraically closed field that, given a point $O \in E(K)$, there is a bijection

$$\sigma : Pic^0(E) \to E$$

which is induced by $\tilde{\sigma} : \mathrm{Div}^0(E) \to E \ ; \ D \mapsto p$ where p is the unique point of E such that the divisor (D) is linearly equivalent to $(p) - (O)$. Thus, the natural group structure on $Div(E)$ will induce one on

E itself. That this is the same group law on E defined geometrically, is the contention of the following result:

Lemma *With notations as above, let $\theta : E \to Pic^0(E)$ denote the map σ^{-1} i.e., $\theta(p)$ is the class of $(p)-(O)$. Then, for any $p, q \in E$, $\theta(p \oplus q) = \theta(p) + \theta(q)$ where $\oplus$ is the geometric group law on E.*

Proof: Let $L \subset \mathbb{P}^2$ be the line $F(X,Y,Z) = \alpha X + \beta Y + \gamma Z = 0$ through p, q. If r is the third point of the intersection $L \cap E$, then let us write $G(X,Y,Z) = \alpha' X + \beta' Y + \gamma' Z = 0$ for the line L' joining r and O. Since $Z = 0$ intersects E at O with multiplicity 3, we have from the definition of $\oplus$ that $div(F/Z) = p+q+r-3(O)$ and $div(G/Z) = r+(p \oplus q)-2(O)$. Thus, $(p \oplus q) - p - q + O = div(G/F) \sim 0$ in $Div^0(E)$. This proves that $\theta(p \oplus q) - \theta(p) - \theta(q) = 0$ in $Pic^0(E)$.

Finally, on curves (or, more generally on varieties of any dimension), there is the notion of differentials which is extremely useful.

Definition For any field K, a K-algebra A and an A-module M, one defines a *derivation* to be a K-linear map $D : A \to M$ satisfying $D(ab) = aD(b) + bD(a)$.

It is easy to prove that given a K-algebra A, there is a unique (up to isomorphism) A-module $\Omega_K(A)$ and a derivation $d : A \to \Omega_K(A)$ such that the image of d generates $\Omega_K(A)$ as an A-module and any derivation $D : A \to M$ factors through a unique A-linear map from $\Omega_K(A)$ to M. In fact, if $x_1, \cdots, x_n$ generate A as a K-algebra, then $dx_1, \cdots, dx_n$ generate $\Omega_K(A)$ as an A-module. $\Omega_K(A)$ is called the *module of K-differentials of A*. When A is the function field $K(V)$ of a variety V, then one also calls $\Omega_K(K(V))$ the module of K-differentials of the variety V. One also calls its elements *differential 1-forms on V*. The basic fact is :

Proposition *Let V be a variety of dimension n over an algebraically closed field K. Then, $\Omega_K(K(V))$ is a $K(V)$-vector space of dimension n. Moreover, for any nonsingular point p of V, $\Omega_K(\mathcal{O}_p)$ is a free $\mathcal{O}_p$-module of rank n, where $\mathcal{O}_p$ is the local ring at p.*

Further, if p is a point of V, an element in the image under the natural inclusion $\Omega_K(\mathcal{O}_p) \subseteq \Omega_K(K(V))$ is said to be *regular at p*.

If V is a nonsingular curve over an algebraically closed field K, then for any 1-form ω on V and any point p in V, the *order of ω at p* is defined to be the largest n for which $\omega \in t^n \Omega_K(\mathcal{O}_p)$ where t is a uniformising parameter for $\mathcal{O}_p$. In this sense, one talks about the order of zeroes and

of poles for an 1-form. We shall soon see that for elliptic curves, there is an essentially unique 1-form which has neither zeroes nor poles.

4. Elliptic Curves - Definition

An elliptic curve over a field K is a non-singular, projective plane curve of genus 1 having a specified base point $O \in E(K)$. In simpler language, an elliptic curve is the set of solutions in $\mathbb{P}^2(K)$ of an equation of the form $Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3$ with $a_i \in K$, with one of three partial derivatives is non zero at any given solution. If char $K \neq 2, 3$, then an elliptic curve can also be described as the set of solutions set $\mathbb{P}^2(K)$ of an equation of the form $Y^2Z = X^3 + aXZ^2 + bZ^3$, where the cubic $X^3 + aX + b$ has distinct roots. That the first definition implies the second can be proved using the Riemann-Roch theorem. In the last definition, a canonical point $O \in E(K)$ is the "point at infinity" $(0, 1, 0)$.

An elliptic curve is not an ellipse. The name comes from the fact that these equations arise when one tries to measure the perimeter of an ellipse. The above form of the equation is known as the Weierstrass form. Let us assume that characteristic of K is $\neq 2, 3$ for simplicity of notation. We have then:

Theorem
(i) *$E(a, b) : Y^2Z = X^3 + aXZ^2 + bZ^3$ defines an elliptic curve over K (with $O = (0, 1, 0) \in \mathbb{P}^2(K)$) if, and only if, $a, b \in K$ and $4a^3 + 27b^2 \neq 0$.*
(ii) *Every elliptic curve over K is isomorphic to $E(a, b)$ for some $a, b \in K$.*
(iii) *An elliptic curve over K is isomorphic to the curve $E(a, b)$ if, and only if, there exists $t \in K^*$ such that its Weierstrass form can be written as $Y^2Z = X^3 + t^4aXZ^2 + t^6bZ^3$.*

One defines the j-invariant of $E(a, b)$ to be $j(E) = 1728\frac{4a^3}{4a^3+27b^2}$. Note that by (iii) of the above theorem, it makes sense to define $j(E) = j(E(a, b))$ if E is isomorphic to $E(a, b)$. Here is an important fact (again with the assumption that $K = \bar{K}$) : *$j(E) = j(E')$ if, and only if, $E \cong E'$.*

Let $\mathbb{C}$ be the field of complex numbers. If E is an elliptic curve over $\mathbb{C}$ then $E(\mathbb{C})$ can also be thought of complex manifold of dimension one. Thus, $E(\mathbb{C})$ is a compact Riemann surface of genus one and hence $E(\mathbb{C})$ is just a complex torus of dimension one. i.e., $\mathbb{C}/\Lambda$ where Λ is a lattice

in $\mathbb{C}$. This follows from the classical theory of elliptic functions. In other words, there is an isomorphism of Riemann surfaces $E(\mathbb{C})$ and $\mathbb{C}/\Lambda$.
For an elliptic curve $E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ over any field, there exists a differential 1-form ω which is invariant under all translations T_p i.e., $T_p^*\omega = \omega$ for all $p \in E$. This is called an invariant differential; it is unique up to a scalar multiple. One can write $\omega = \frac{dx}{2y+a_1x+a_3}$. It is also seen to have no zeroes or poles; that is, its order at every point is zero.

5. Torsion points of Elliptic curves and Isogenies

Let K be a field and E be an elliptic curve defined over K. A point p of $E(K)$ such that $[n](p) = O$, for some integer $n \geq 1$, is called a torsion point of E over K. Here, we have denoted by $[n]p$ the point $p + \cdots + p$ added n times (if $n \geq 0$) or the inverse of the point $p + \cdots + p$ added $-n$ times (if $n < 0$). If E is an elliptic curve over a field $K = \bar{K}$, and $n \neq 0$, then the *n-torsion subgroup* is defined as

$$E[n] := \{p \in E(K) : [n]p = O\}.$$

One has:
If $n \neq 0$ is not a multiple of the characteristic of K, then

$$E[n] \cong \mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}.$$

Over an algebraically closed field whose characteristic divides n, it can happen that $E[n]$ is not as above (see B. Sury's article [*Su*] in this volume.)
Also, over a field K which is not algebraically closed, the group of n-torsion can be different (of course, it must be a subgroup of the above group).

Remarks
(i) If E is an elliptic curve defined over $\mathbb{R}$, then one may consider $E(\mathbb{R}) \cap E[n]$. It turns out that this is either a cyclic group or it is isomorphic to $\mathbb{Z}/2 \times \mathbb{Z}/2m$ for some $2m$ dividing n. This can be seen quite easily on using the Weil pairing (defined in § 7) and the fact that ± 1 are the only roots of unity in $\mathbb{R}$.
(ii) If E is an elliptic curve defined over $\mathbb{Q}$, then the subgroup $E(\mathbb{Q})_{tor}$ of all points of finite order in $E(\mathbb{Q})$ is a finite group (by the Mordell-Weil theorem). Using (i), it is either a cyclic group or it is isomorphic to $\mathbb{Z}/2 \times \mathbb{Z}/2m$ for some m.

(iii) It is a far more difficult problem to determine which subgroups of $\mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$ occur as *n-torsion subgroups* of an elliptic curve over K. For example, Mazur proved that over $\mathbb{Q}$, only finitely many (exactly 15) groups can occur as torsion groups.
(iv) Over general number fields K, it is a result of Merel that the order of the torsion group $E(K)_{tor}$ is bounded purely in terms of the degree $[K : \mathbb{Q}]$.

We saw in the above discussion that for each integer n and any elliptic curve E, there is a map $[n] : E(K) \to E(K)$ defined by $p \mapsto [n]p$. This is an example of an isogeny, when $n \neq 0$. Let us define this notion now.

A non constant morphism $\phi : E_1 \to E_2$ between elliptic curves E_1 and E_2 such that $\phi(O) = O$ is called an isogeny.

Therefore, an isogeny must be surjective and must have finite kernel. In fact, the rigidity theorem implies: *An isogeny is a group homomorphism.*

To see this, look at $\theta : E_1 \times E_1 \to E_2$ defined as $\theta(x, y) = \phi(x + y) - \phi(x) - \phi(y)$. Since $\phi(O) = O$, we have $\theta(E_1 \times \{O\}) = \{O\}$. By rigidity, there exists $\psi : E_1 \to E_2$ such that $\theta(x, y) = \psi(y)$ for all $x \in E_1$. As $\theta(O, y) = O$, $\forall y$ one has $\psi \equiv O$ i.e., $\theta \equiv 0$.

Moreover, as a trivial consequence of the fact about the fibres of a morphism of curves, we see that, if $\phi : E_1 \to E_2$ is an isogeny, then, $\#\ \mathrm{Ker}\phi = \deg_{sep} \phi$.

One writes $\mathrm{Hom}(E_1, E_2)$ for the group of isogenies from E_1 to E_2 together with constant map O.

For $E_1 = E_2 = E$ (say), this group is in fact a ring ,with composition as multiplication, called the *endomorphism ring* of E and is denoted by $\mathrm{End}(E)$. This ring has many important properties. In the next section, we shall recall some properties of the ring $\mathrm{End}(E)$.

One has also the following important result on isogenies:

Theorem *Let $\phi : E_1 \to E_2$ be an isogeny. Then, there is a unique isogeny $\hat{\phi} : E_2 \to E_1$ satisfying $\hat{\phi} \circ \phi = [\deg \phi]$. $\hat{\phi}$ is called the dual of ϕ.*

Sketch of proof: For two isogenies ϕ_1, ϕ_2 from E_2 to E_1 satisfying

$$\phi_1 \circ \phi = [\deg \phi] = \phi_2 \circ \phi$$

one has $(\phi_1 - \phi_2) \circ \phi = [0]$ which implies that $\phi_1 - \phi_2 = 0$ since ϕ is surjective. The uniqueness follows thus.

To show the existence of $\hat{\phi}$, for simplicity, we shall describe it when ϕ is separable. By the above remark, we have in this case $\deg \phi = \text{Ker}\phi = n$, say. Now, $\text{Ker}\phi \subseteq \text{Ker}[n]$. The isogeny ϕ gives rise to the injection $\phi^* : K(E_2) \to K(E_1)$. This gives a Galois extension $K(E_1)$ over $\phi^* K(E_2)$ with the Galois group equal to $\text{Ker}\phi$. (We have written K for the underlying field over which E_i are defined). Similarly, the injection $[n]^* : K(E_1) \to K(E_2)$ gives a Galois extension with Galois group $\text{Ker}[n]$. By Galois theory, there exists an injection $\psi^* : K(E_1) \to K(E_2)$ such that $\phi^* \circ \psi^* = [n]^*$. The corresponding $\psi : E_2 \to E_1$ can be taken to be the required dual isogeny $\hat{\phi}$.

Here are some facts on duals and degrees of isogenies which will turn out to be very useful: If $\phi, \psi : E_1 \to E_2$ are isogenies then
(i) $\widehat{\phi + \psi} = \hat{\phi} + \hat{\psi}$
(ii) $\widehat{[n]} = [n]$
(iii) $\deg[n] = n^2$
(iv) $\deg \hat{\phi} = \deg \phi$
(v) $\hat{\hat{\phi}} = \phi$
(vi) $\deg(-\phi) = \deg \phi$.
(vii) The function

$$d : \text{Hom}(E_1, E_2) \times \text{Hom}(E_1, E_2) \to \mathbb{Z}$$

defined by $d(\phi, \psi) := \deg(\phi+\psi) - \deg \phi - \deg \psi$ is symmetric and bilinear,
(viii) $\deg \phi > 0$ for any isogeny ϕ.

Proofs of some parts: We do not prove (i) here. The proof is a bit involved and essentially uses the lemma in § 3 which follows the Riemann-Roch theorem; an element $\sum [n_i]p_i$ of an elliptic curve E is O if, and only if, the corresponding divisor $\sum n_i p_i$ is the divisor of a rational function on E.
(ii) follows by induction on $|n|$ on using (i). (iii) is due to the fact that $\widehat{[n]} = [n]$ and $[n] \circ [n] = [n^2]$. To prove (iv), write $n = \deg \phi$. Then, $[n^2] = [\deg[n]] = [\deg(\hat{\phi} \circ \phi)] = [\deg \hat{\phi} \deg \phi] = [n \deg \hat{\phi}]$. Thus, $n = \deg \hat{\phi}$. For (v) again, write $n = \deg \phi$. Then,

$$\hat{\phi} \circ \phi = [n] = \widehat{[n]} = \widehat{(\hat{\phi} \circ \phi)} = \hat{\phi} \circ \hat{\hat{\phi}}$$

which gives (v). To prove (vii), note that if $\phi, \psi : E_1 \to E_2$, then

$$[d(\phi, \psi)] = [\deg(\phi + \psi)] - [\deg(\phi)] - [\deg(\psi)]$$

$$= (\widehat{\phi+\psi}) \circ (\phi+\psi) - \hat{\phi} \circ \phi - \hat{\psi} \circ \psi$$
$$= (\hat{\phi}+\hat{\psi}) \circ (\phi+\psi) - \hat{\phi} \circ \phi - \hat{\psi} \circ \psi$$
$$= \hat{\phi} \circ \psi + \hat{\psi} \circ \phi,$$

and the last expression is symmetric and bilinear.

6. Tate modules, ℓ-adic representations and complex multiplication

Let E be an elliptic curve defined over K. Suppose ℓ is a prime different from the characteristic of K. We know that the ℓ^n-division points of E over $\bar{K}$(i.e., $E[\ell^n] = \mathrm{Ker}[\ell^n]$) is $\simeq \mathbb{Z}/\ell^n \times \mathbb{Z}/\ell^n$. The inverse limit of the groups $E[\ell^n]$ with respect to the maps $E[\ell^{n+1}] \xrightarrow{[\ell]} E[\ell^n]$ is the *Tate module* $T_\ell(E) = \varprojlim E[\ell^n]$. Since each $E[\ell^n]$ is naturally a $\mathbb{Z}/\ell^n$-module, it can be checked that $T_\ell(E)$ is a $\mathbb{Z}_\ell (= \varprojlim \mathbb{Z}/\ell^n)$-module. It is clearly a free $\mathbb{Z}_\ell$-module of rank 2.

Evidently, any isogeny $\phi : E_1 \to E_2$ induces a $\mathbb{Z}_\ell$-module homomorphism $\phi_\ell : T_\ell(E_1) \to T_\ell(E_2)$. In particular, we have a representation: $\mathrm{End}(E) \to M_2(\mathbb{Z}_\ell)$; $\phi \mapsto \phi_\ell$. Note that $\mathrm{End}(E) \hookrightarrow \mathrm{End}(T_\ell(E))$ is injective because if $\phi_\ell = 0$, then ϕ is 0 on $E[\ell^n]$ for all large n i.e., $\phi = 0$.

For an elliptic curve E over K the endomorphism $[\ell^n]$ is defined over K. Hence, there is an action of $\mathrm{Gal}(\bar{K}/K)$ on $E[\ell^n]$ for all $n \geq 0$. The action of $\mathrm{Gal}(\bar{K}/K)$ on the various $E[\ell^n]$ gives a 2-dimensional representation

$$\rho_{E,\ell} : Gal(\bar{K}/K) \to Aut(T_\ell(E)) \cong GL_2(\mathbb{Z}_\ell) \subset GL_2(\mathbb{Q}_\ell),$$

which is called the *ℓ-adic* representation of the Galois group $Gal(\bar{K}/K)$ attached to E.

For K finite or an algebraic number field, there are deep theorems due to Tate and Faltings, respectively, which assert that *two elliptic curves E_1 and E_2 over K are isogenous if, and only if, the corresponding ℓ-adic representations are isomorphic for all ℓ coprime to* $\mathrm{Char}(K)$.

Recall that the isogenies from an elliptic curve E to itself form a ring $\mathrm{End}(E)$ and $n \mapsto [n]$ induces an injective ring homomorphism $[\ ] : \mathbb{Z} \to \mathrm{End}(E)$. An elliptic curve E is said to have *complex multiplication* if $\mathrm{End}(E) \ncong \mathbb{Z}$.

Examples
(i) The curve $y^2 = x^3 + x$ has complex multiplication viz., $x \mapsto -x, y \mapsto$

iy where i is a square root of -1.
(ii) $y^2 = x^3 + 1$ has complex multiplication, namely, $(x, y) \mapsto (\omega x, y)$ where ω is a primitive 3rd root of unity.

The only possibilities for End(E) are given by the following result:

Proposition
(i) End(E) has no zero divisors.
(ii) End(E) is torsion-free.
(iii) End(E) is either $\mathbb{Z}$, or an order in an imaginary quadratic field over $\mathbb{Q}$ or an order in a quaternion division algebra over $\mathbb{Q}$

Remarks
(i) End(E) has char. 0 no matter what field E is defined over !
(ii) If Char.$K = 0$, then for any elliptic curve E over K, End E must be either $\mathbb{Z}$ or an order in an imaginary quadratic field.

Before proving the proposition, let us see what it means for E over $\mathbb{C}$. Let $\lambda : \mathbb{C}/\langle 1, \tau\rangle \to \mathbb{C}/\langle 1, \tau\rangle$ be an isogeny $\ncong [n]$. Then λ is multiplication by a complex number, say, λ again. Then $\lambda \cdot 1, \lambda \cdot \tau \in \mathbb{Z} + \mathbb{Z}\tau$.

$$\lambda = a + b\tau, \lambda\tau = c + d\tau.$$

Since we are assuming $\lambda \notin \mathbb{Z}, b \neq 0$. Now $(a + b\tau)\tau = c + d\tau$ gives a quadratic equation for τ i.e., $\tau \in K := \mathbb{Q}(\sqrt{d})$ for some d. Since $Im(\tau) > 0, \tau \notin \mathbb{R}$ i.e., K is an imaginary quadratic field. Further, $\mathbb{Q}(\lambda) = \mathbb{Q}(a + b\tau) = \mathbb{Q}(\tau) = K$. Thus, End$(E)$ is an order in an imaginary quadratic field if End$(E) \ncong \mathbb{Z}$.

Let us prove the proposition now.

Proof of Proposition: First, we shall prove for elliptic curves E_1, E_2 that Hom(E_1, E_2) is torsion free, and that End(E) has no zero divisors. Suppose $\phi : E_1 \to E_2$ is an isogeny and $[n] \circ \phi = [0]$. Then compare degrees to get $n^2 \deg \phi = 0$. If $[n] \neq [0]$, then we get $\deg \phi = 0$. This is a contradiction. The other assertion is completely similar. Now, we shall discuss the structure of End(E) and prove part (iii).
Note that any $\phi \in$ End(E) satisfies a monic polynomial of degree 2 over $\mathbb{Z}$ viz., the polynomial $f(X) = (X - \phi)(X - \hat{\phi})$. Look at $A =$ End$(E) \otimes_{\mathbb{Z}} \mathbb{Q}$. If $A \neq \mathbb{Q}$, choose $\alpha \in A \setminus \mathbb{Q}$. Note that $\alpha - \frac{tr(\alpha)}{2} \in A \setminus \mathbb{Q}$ and so we may assume $tr(\alpha) = 0$. Now $\alpha^2 < 0$. So, $\mathbb{Q}(\alpha)$ is an imaginary quadratic field. If $A \neq \mathbb{Q}(\alpha)$, let $\beta \in A \setminus \mathbb{Q}(\alpha)$. As $\beta - \frac{tr(\beta)}{2} - \frac{tr(\alpha\beta)}{2\alpha^2}\alpha \in A \setminus \mathbb{Q}(\alpha)$, we may assume that

$$tr(\beta) = 0 = tr(\alpha\beta).$$

So, $tr(\alpha) = 0 = tr(\beta) = tr(\alpha\beta)$ gives

$$-(\alpha\beta) = \widehat{(\alpha\beta)} = \hat{\beta}\hat{\alpha} = (-\beta)(-\alpha) = \beta\alpha.$$

Hence, $A' = \mathbb{Q}[\alpha, \beta] = \mathbb{Q} + \mathbb{Q}\alpha + \mathbb{Q}\beta + \mathbb{Q}\alpha\beta$ is a quaternion algebra. Suppose $A \neq A'$; let $\gamma \in A \backslash A'$. Then $\gamma - \frac{tr(\gamma)}{2} + \frac{tr(\alpha\gamma)}{2\alpha^2}\alpha + \frac{tr(\beta\gamma)}{2\alpha^2}\beta \in A \backslash A'$. We may assume $tr(\alpha\gamma) = tr(\beta\gamma) = 0$. Thus, $\alpha\gamma = -\gamma\alpha, \beta\gamma = -\gamma\beta$. So $\alpha \cdot \beta\gamma = -\alpha\gamma\beta = \gamma\alpha\beta = -\gamma\beta\alpha = \beta\gamma\alpha$ i.e., α and $\beta\gamma$ commute. But, then the algebra generated by α and $\beta\gamma$ is a field since it has no zero divisors and the inverses (which exist by positive definiteness) are in the subalgebra generated by α and $\beta\gamma$. Since $\gamma \notin \mathbb{Q}[\alpha, \beta], \beta\gamma$ also $\notin \mathbb{Q}[\alpha]$ i.e., A contains a field extension of degree 4 over $\mathbb{Q}$ i.e., $\exists\theta \in A$ which has degree 4 over $\mathbb{Q}$. This contradicts the first observation that each element of A satisfies a quadratic equation over $\mathbb{Q}$. Thus, $A = A' = \mathbb{Q}[\alpha, \beta]$, a quaternion division algebra over $\mathbb{Q}$.

7. The Weil pairing

Let K be a field and ℓ be prime number coprime to Char(K). We denote by μ_{ℓ^n} the the subgroup $\{\zeta : \zeta^{\ell^n} = 1\}$ of $\bar{K}^*$, where $\bar{K}^*$ is the multiplicative group of all non-zero elements of $\bar{K}$. Note that, if $T_\ell(\mu) = \varprojlim \mu_{\ell^n}$ then $T_\ell(\mu) \cong \mathbb{Z}_\ell$.

Let E be an elliptic curve over K. The *Weil pairing* is a non-degenerate, bilinear, alternating pairing

$$e : T_\ell(E) \times T_\ell(E) \to T_\ell(\mu)$$

satisfying $e(\phi x, y) = e(x, \hat{\phi} y)$ for all $\phi \in \mathrm{End}(E)$. The Weil pairing e is made up from maps $e_n : E[\ell^n] \times E[\ell^n] \to \mu_{\ell^n}$ and can be defined via divisors as done below. Before that, a brief word about how e can be described over $\mathbb{C}$. For $E(\mathbb{C}) = \mathbb{C}/L$ over $\mathbb{C}$, there are two descriptions. The first one is to write $L = \mathbb{Z} + \mathbb{Z}\tau$ with $\mathrm{Im}\tau > 0$. Then

$$e(a\tau + b, c\tau + d)) = ad - bc.$$

Then, by the fact that $T_\ell(E(\mathbb{C}))$ is isomorphic to $L \otimes_{\mathbb{Z}} \mathbb{Z}_\ell$, we get a description of the Weil pairing e. The other is to view L as $H_1(E(\mathbb{C}), \mathbb{Z})$ and e_n is the homology intersection pairing on the real surface $E(\mathbb{C})$ with $\mathbb{Z}/\ell^n$ coefficients. As above this gives Weil pairing e on $T_\ell(E(\mathbb{C}))$. Let us describe e in general now. Using the Riemann-Roch theorem, it is a nice little exercise to see that for $p_1, \ldots, p_k \in E(\bar{K})$ the divisor $\sum n_i p_i$

is the divisor of a function if, and only if, $\sum n_i = 0$ and $\sum [n_i]p_i = O$ in $E(\bar{K})$. Let $m \geq 1$ be an integer coprime to char(K) and $t \in E[m]$. Then $\exists\ f \in \bar{K}(E)$ such that $(f) = m(t) - m(O)$. If $t' \in E$ with $[m]t' = t$, then $\exists\ g \in \bar{K}(E)$ with

$$(g) = \sum_{r \in E[m]} (t' + r) - \sum_{r \in E[m]} (r)$$

(note $\#E[m] = m^2$ and $m^2 t' = 0$). Thus, $f \circ [m]$ and g^m have the same divisor. Multiplying f by an element of $\bar{K}^*$, we may, without loss of generality, assume $f \circ [m] = g^m$. Let $\mu_m = \{\zeta \in \bar{K}^* : \zeta^m = 1\}$. Define $e_m : E[m] \times E[m] \to \mu_m$ by

$$e_m(s,t) \mapsto \frac{g(x+s)}{g(x)},$$

where x is any point such that $g(x+s), g(x)$ are both defined and non-zero. Notice that the image indeed belongs to μ_m as $g(x+s)^m = (f \circ [m])(x+s) = (f \circ [m])(x) = g(x)^m$. Although g is defined only up to multiplication by an element of $\bar{K}^*$, the ratio is independent of its choice. That the choice of x is immaterial, is known as Weil reciprocity. The Weil pairing has the following properties:

(a) e_m is bilinear
(b) e_m is skew-symmetric
(c) e_m is non-degenerate
(d) e_m is Gal $(\bar{K}/K)$- invariant i.e., $e_m(s^\sigma, t^\sigma) = e_m(s,t)^\sigma$.
(e) $e_{mn}(s,t) = e_m([n]s, t)$ if $s \in E[mn], t \in E[m]$.
(f) e_m is surjective.

The most important property of e_m is proved in the following :

Proposition *Let $s \in E_1[m], t \in E_2[m]$ and let $\phi : E_1 \to E_2$ be an isogeny. Then, $e_m(s, \hat{\phi}(t)) = e_m(\phi(s), t)$.*

Proof: Let $(f) = m(t) - m(O)$ and $f \circ [m] = g^m$ as before. Then, $e_m(\phi(s), t) = \frac{g(x+\phi(s))}{g(x)}$. Choose $h \in \bar{K}(E_1)$ such that

$$(\hat{\phi}(t)) - (O) + (h) = \phi^*((t)) - \phi^*((O)),$$

where $\phi^* : \mathrm{Div}(E_2) \to \mathrm{Div}(E_1)$ is the map defined by $p \mapsto \sum_{\{q:\phi(q)=p\}} e_q(\phi) q$. The right hand side is, by definition, equal to

$$\deg_{insep}(\phi) \left(\sum_{w \in \mathrm{Ker}\phi} (t_0 + w) - \sum_{w \in \mathrm{Ker}\phi} w \right)$$

for any $t_0 \in \phi^{-1}(t)$.

Now $((f \circ \phi)/h^m) = \phi^*(f) - m(h) = m(\hat{\phi}(t)) - m(O)$.
Hence,

$$(\frac{g \circ \phi}{h \circ [m]})^m = \frac{f \circ [m] \circ \phi}{(h \circ [m])^m} = \frac{f \circ \phi}{h^m} \circ [m].$$

So, from the definition of e_m,

$$e_m(s, \hat{\phi}(t)) = \frac{\frac{g \circ \phi}{h \circ [m]}(x+s)}{\frac{g \circ \phi}{h \circ [m]}(x)}$$

$$= \frac{g(\phi(x)+\phi(s))}{g(\phi(x))} \frac{h([m]x)}{h([m]x+[m]s)}$$

$$= \frac{g(\phi(x)+\phi(s))}{g(\phi(x))} = e_m(\phi(s), t).$$

8. Elliptic curves over number fields

The first main theorem over number fields K is the Mordell-Weil theorem which asserts that $E(K)$ *is a finitely generated Abelian group for an elliptic curve* E *over* K.
Elliptic curves arise naturally often in the context of classical number-theoretic problems like the so-called congruent number problem. One defines a natural number d to be a *congruent number* if there is a right-angled triangle with rational sides and area d. For example, 6 and 157 are congruent numbers. The following shows the connection with elliptic curves:

Lemma *Let* d *be a natural number. Then,* d *is a congruent number if, and only if, the elliptic curve* $E_d : y^2 = x^3 - d^2x$ *has a* $\mathbb{Q}$*-rational point* (x, y) *with* $y \neq 0$.

Proof: Let $u \leq v \leq w$ be the sides of a right triangle with rational sides. Let d be the area $\frac{1}{2}uv$. Then, $P = (\frac{d(u-w)}{2}, \frac{2d^2(u-w)}{v^2}) \in E_d(\mathbb{Q})$. Conversely, if $P = (x, y) \in E_d(\mathbb{Q})$ be such that $y \neq 0$. Then, $u = |\frac{x^2-d^2}{y}|, v = |\frac{2dx}{y}|, w = |\frac{x^2+d^2}{y}|$ gives a right triangle with rational sides and area d.
A connection with the Fermat's two-squares theorem (namely, every prime $p \equiv 1 \bmod 4$ is a sum of two squares) can be seen already in Gauss's study of the elliptic curve $E : y^2 = x^3 - x$. For each prime p, let N_p be the cardinality of the set $\{(x, y) : 0 \leq x, y \leq p-1\ ,\ y^2 \equiv$

$x^3 - x \ mod \ p\}$. Gauss proved that $N_2 = 2$, $N_p = p$ if $p \equiv 3 \bmod 4$, and $N_p = p - 2r$ if $p \equiv 1 \bmod 4$ where $p = r^2 + s^2$ with r odd and $r + s \equiv 1 \bmod 4$.

Loosely speaking, if an elliptic curve E over $\mathbb{Q}$ has a nice pattern of N_p's (as in the curve $y^2 = x^3 - x$ studied by Gauss), one finds that E comes from a modular form. The Shimura-Taniyama-Weil conjecture (see below) - proved completely now - asserts that this is true for any elliptic curve over $\mathbb{Q}$.

Given an elliptic curve E over a number field K, one can look at the nonsingular points E_{ns} of the curve obtained by "reducing modulo prime ideals". The *L-function* of E over K encodes information about the number of points that the reduced curve has over the various finite fields; it is a Dirichlet series defined by an Euler product. For E over $\mathbb{Q}$, this looks like

$$L(E,s) = \prod_{p|N} \left(1 - \frac{a_p}{p^s}\right)^{-1} \prod_{p \not| N} \left(1 - \frac{a_p}{p^s} + \frac{1}{p^{2s-1}}\right)^{-1},$$

where N is an integer known as the conductor of E and $a_p = p + 1 - |E_{ns}(\mathbb{F}_p)|$ for each prime p. It is not hard to prove that isogenous curves over $\mathbb{Q}$ have the same L-function. The famous Birch and Swinnerton-Dyer conjecture asserts that for E over $\mathbb{Q}$, *the L-function $L(E,s)$ defined above extends to an entire function and its order at $s = 1$ is precisely the rank of the Mordell-Weil group $E(\mathbb{Q})$.*

We end with a famous conjecture which is now solved.

Shimura-Taniyama-Weil Conjecture : *If E is an elliptic curve defined over $\mathbb{Q}$, then there exists $N > 0$ and a non constant $\mathbb{Q}$-morphism $F : X_0(N) \to E$.*

Here, the so-called modular curve $X_0(N)$ is the projective curve defined over $\mathbb{Q}$ whose $\mathbb{C}$-points are obtained by compactifying the Riemann surface $\Gamma_0(N)\backslash\mathcal{H}$ where $\Gamma_0(N) := \{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) : c \equiv 0 \ mod \ N\}$. The conjecture was solved for semi stable curves by Taylor and Wiles and was enough to give Fermat's last theorem as a consequence. Now, it has been solved in its full generality by Breuil, Conrad, Diamond and Taylor.

We end with the remarkable statement that $e^{\pi\sqrt{163}}$ *is almost an integer.* A popular myth credits Ramanujan with this but the authors have not

been able to verify the veracity of this attribution. One computes to find that

$$e^{\pi\sqrt{163}} = 262537412640768743.9999999999992\cdots(!)$$

Here is the explanation.
Look at the Fourier expansion of the j-function

$$j(\tau) = \frac{1}{q} + 744 + 196884q + \cdots\cdots$$

where $q = e^{2\pi i\tau}$. From the theory of complex multiplication, it follows that for $\tau = \frac{1+\sqrt{-d}}{2}$, the number $j(\tau)$ is an algebraic integer of degree equal to the class number of the imaginary quadratic field $\mathbb{Q}(\sqrt{-d})$. There are only finitely many imaginary quadratic fields with class number 1; the largest such d is 163. Thus, $j(\frac{1+\sqrt{-163}}{2}) \in \mathbb{Z}$. Feeding this in the Fourier expansion and noting that $q = e^{-\pi\sqrt{163}}$, we get that $\frac{1}{q} = e^{\pi\sqrt{163}}$ is very close to the integer $j(\frac{1+\sqrt{-163}}{2}) + 744$ as the terms involving positive powers of q are small.

References

[*C*] J.W.S. Cassels, *Lectures on elliptic curves*, London Mathematical Society Student Texts **24**, Cambridge University Press 1991.

[*M*] C. Musili, *Algebraic-geometry for beginners*, Texts and Readings in Mathematics Vol. **20**, Hindustan Book Agency, New Delhi 2001.

[*S*] J. H. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics **106**, Springer-Verlag, New York 1986.

[*Su*] B. Sury, *Elliptic Curves over Finite Fields*, this volume.

(D. S. Nagaraj) Institute of Mathematical Sciences, CIT Campus, Taramani, Chennai 600 113, India.

(B. Sury) Stat-Math Unit, Indian Statistical Institute, Bangalore 560 059, India.

E-mail address, D. S. Nagaraj: `dsn@imsc.res.in`

E-mail address, B.Sury: `sury@isibang.ac.in`