Mathematisch Instituut
Universiteit van Amsterdam
Roetersstraat 15
1018 WB Amsterdam

ELLIPTIC CURVES AND FACTORIZATION ALGORITHMS

Jurriaan van der Lingen

Report 87-2

Received January 1987

ELLIPTIC CURVES AND FACTORIZATION ALGORITHMS.

Version 1 - January 1987.

Jurriaan van der Lingen

Contents.

Preface.

These notes grew out of a course given by H.W. Lenstra, Jr. at the University of Amsterdam in the fall semester of 1986. They are meant to give an introduction to the theory of elliptic curves to non-specialists, and to review some of the recent applications to number theoretic algorithms. The prerequisites are kept to a minimum. In fact, apart from a few execises which are not essential for the understanding of the main text, a basic knowledge of groups, fields and rings will suffice. In particular no results from algebraic geometry are used. Some statements are given without proof. With the exception of theorem (4.6)* this is done to avoid a lengthy exposition rather than mathematical difficulties. The references for proofs are all easily accessible to the average student. Our main reference is Silverman [19] who based his book on a survey article of Tate [20]. A history of elliptic curves and Diophantine equations is given by Bashmakova [2]. Recently a book of Husemöller [7a] has appeared. I would like to stress that since this is a first version of many to follow, suggestions and mild criticism are always welcome.

Notation.

The symbols $\mathbf{Z}, \mathbf{Q}, \mathbf{R}, \mathbf{C}$ and $\mathbf{F}_q$ are used to denote the ring of integers, the fields of rational, real and complex numbers and the finite field of q elements respectively. If K is a field, then $\overline{K}$ denotes the algebraic closure of K.

Acknowledgement.

I am greatly indebted to Hendrik Lenstra for his stimulating support during the preparation of these notes.

JvdL

* An elementary proof of theorem (4.6) will be given in the following version.

§1. The group law on an elliptic curve.

Let K be a field. The *projective plane* over K, denoted $\mathbf{P}^2(K)$, is defined as the set of triples $(x,y,z) \in K \times K \times K$, such that x, y and z are not all 0, modulo the equivalence relation given by

$$(x,y,z) \sim (x',y',z') \text{ if there exists } \lambda \in K^* \text{ with } x = \lambda x',\ y = \lambda y',\ z = \lambda z'.$$

The equivalence-class of (x,y,z) under this relation is denoted by $(x:y:z)$. The projective plane is the disjoint union of the affine plane,

$$\mathbf{A}^2(K) = \{ (x:y:z) \in \mathbf{P}^2(K) \mid z \neq 0 \} = \{ (x:y:1) \mid x,y \in K \},$$

and the projective line at ∞,

$$\mathbf{P}^1(K) = \{ (x:y:z) \in \mathbf{P}^2(K) \mid z = 0 \}.$$

In the language of algebraic geometry one can give two definitions for an elliptic curve $E(K)$. According to one definition an elliptic curve is a non-singular plane cubic curve, with a fixed point $O \in E(K)$. An intrinsic definition describes an elliptic curve as a non-singular complete curve of genus 1, again with a fixed point $O \in E(K)$.

In Silverman [19, chapters I-III] one can find the meaning of all this and a proof that the two definitions are equivalent up to isomorphism.

By a suitable choice of coordinates, taking O to be the point (0:1:0) in ∞, one obtains the Weierstrass-form of the equation for an elliptic curve,

$$y^2z + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz^2 + a_6z^3, \tag{1}$$

The inhomogeneous equation is

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6. \tag{2}$$

If char $K \neq 2$ or 3 the equation can be simplified by replacing y by $y - (a_1x + a_3)/2$ and x by $x - (4a_2 + a_1^2)/12$,

$$y^2 = f(x) = x^3 + ax + b. \tag{3}$$

If char $K \neq 2$, a curve given by equation (3) is non-singular if and only if

$$\Delta(f) = -(4a^3 + 27b^2) \neq 0.$$

Here $\Delta(f)$ denotes the discriminant of f. For convenience we shall always assume that K has characteristic $\neq 2$ or 3. This justifies the following definition.

(1.1) **Definition.** Let K be a field of characteristic $\neq 2$ or 3. An *elliptic curve* over K, denoted $E = E_{a,b}$, is a pair $(a,b) \in K \times K$ such that $4a^3 + 27b^2 \neq 0$. The *set of points* of E over K is $E(K) = \{ (x:y:z) \in \mathbf{P}^2(K) \mid y^2z = x^3 + axz^2 + bz^3 \}$. Similarly one defines $E(L)$ for a field extension L of K.

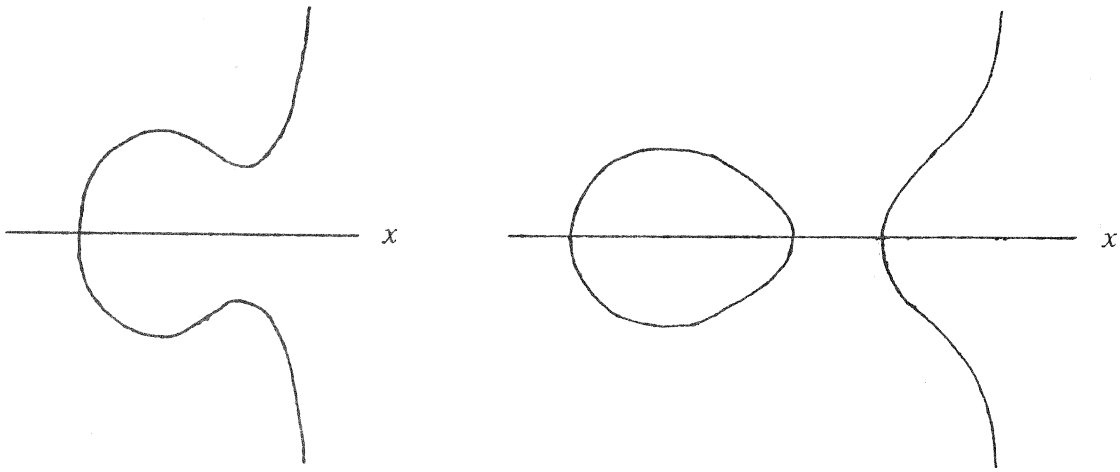
Note that two different elliptic curves may give rise to the same set of points. This can be compared with the difference between a polynomial as a formal expression and as a function.

A linear transformation of (x,y) that turns the equation (3) into a similar equation will always have the form $(x,y) \mapsto (u^2x,u^3y)$, with $u \in K^*$.

(1.2) **Definition.** Let $E_{a,b}$ and $E_{a',b'}$ be elliptic curves over K. An *isomorphism* $E \to E'$ over K is an element $u \in K^*$ satisfying $a' = u^4a$ en $b' = u^6b$.

The identity $\mathrm{id}_E : E \to E$ is $1 \in K$ and if $u : E \to E'$ en $v : E' \to E''$ then uv is the composed map $uv : E \to E' \to E''$. An isomorphism $u : E \to E'$ induces a bijection $E(K) \to E'(K)$ by sending $(x:y:z)$ to $(u^2x:u^3y:z)$.

When $K = \mathbf{R}$, the field of real numbers, (the affine part of) an elliptic curve has one of the following shapes:



Since $\Delta(f) \neq 0$ in (3), f has one or three zeros and the elliptic curve intersects the x-axis once or three times accordingly.

On the set of points of an elliptic curve one can define an abelian group law matching the geometrical structure of the curve, as was remarked by Euler. To be exact: the group operations are morphisms and the curve together with these operations is a *group variety*. We want $O = (0:1:0)$ in ∞ to be the zero element of the group, and three collinear points on $E(K)$ must have a sum equal to O. Combining this we see that the opposite of an element $(x:y:z)$ must be $(x:-y:z)$, since the line through these points intersects the curve at O.

(1.3) **Definition.** The group law on an elliptic curve $E = E_{a,b}$ is given by:

(a) If P (or Q) $= O$, then $P + Q = Q$ (or P) ;

(b) If $P = -Q$, then $P + Q = O$;

(c) If none of the above apply and $P = (x_1:y_1:1)$, $Q = (x_2:y_2:1)$, then

$$P + Q = (x_3 : -(\lambda x_3 + \nu) : 1) \ , \tag{4}$$

with

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1} \quad , \quad \nu = y_1 - \lambda x_1 \quad , \quad x_3 = \lambda^2 - x_1 - x_2 \ , \tag{5}$$

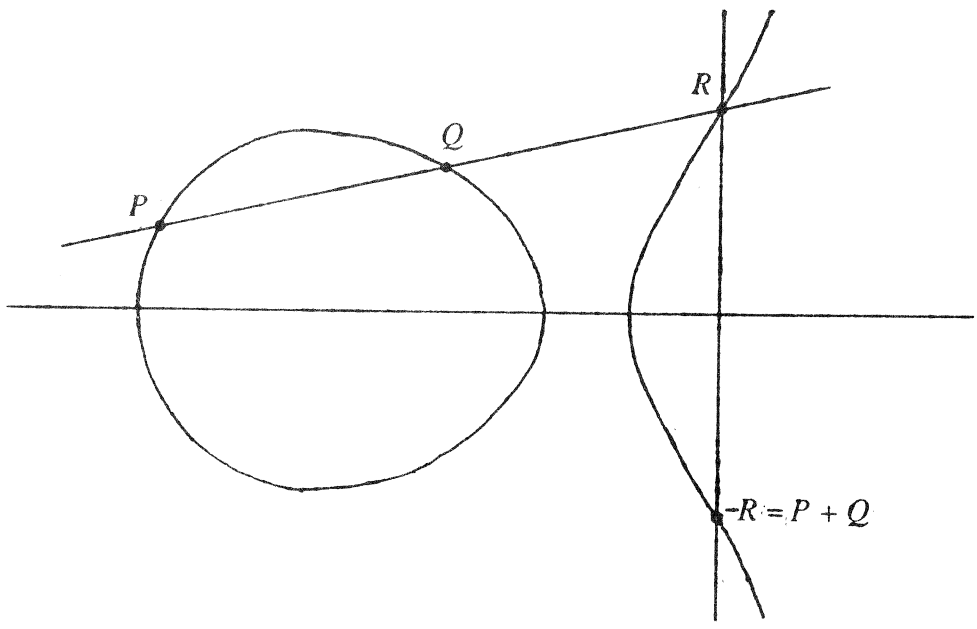
or

$$\lambda = \frac{{x_1}^2 + x_1 x_2 + {x_2}^2 + a}{y_2 + y_1} \quad , \quad \nu = y_1 - \lambda x_1 \quad , \quad x_3 = \lambda^2 - x_1 - x_2. \tag{6}$$

Since $y_i^2 = x_i^3 + a x_i + b$, both values for λ are equal whenever they are both defined. Note that in case (5) we have

$$\begin{aligned} P + Q \quad &= \Big(\frac{(y_2 - y_1)^2}{(x_2 - x_1)^2} - (x_2 + x_1) : \\ &\qquad - \frac{y_2 - y_1}{x_2 - x_1} \left[\frac{(y_2 - y_1)^2}{(x_2 - x_1)^2} - (x_2 + x_1) \right] - \frac{x_2 y_1 - x_1 y_2}{x_2 - x_1} : 1 \Big) \\ &= \big((x_2 - x_1)(y_2 - y_1)^2 - (x_2 + x_1)(x_2 - x_1)^3 : \\ &\qquad -(y_2 - y_1)^3 + (x_2 + x_1)(x_2 - x_1)^2 (y_2 - y_1) - (x_2 y_1 - x_1 y_2)(x_2 - x_1)^2 : \\ &\qquad (x_2 - x_1)^3 \big). \end{aligned}$$

So, after clearing denominators, the formula also makes sense when $x_2 = x_1$, $y_2 \neq y_1$ as well as when $y_2 + y_1 = 0$, ${x_1}^2 + x_1 x_2 + {x_2}^2 + a \neq 0$ in case (6). At least one of the λ is defined when $P \neq -Q$ and P , $Q \neq O$. The affine line through P and Q is $L = \{(x : \lambda x + \nu : 1) \mid x \in K \}$. The intersection points of L with $E(K)$ are given by the zeros in K of $(\lambda x + \nu)^2 - (x^3 + ax + b)$.



This polynomial has three zeros in K (since it already has two: x_1 and x_2), which satisfy $x_1 + x_2 + x_3 = \lambda^2$. So we can give a real-geometric interpretation to the addition as indicated in the figure above.

(1.4) **Theorem.** The algorithm described above induces an abelian group structure on $E(K)$.

A proof of this using the Riemann-Roch theorem can be found in Silverman [19, section III.3]. Hartshorne gives an elegant proof using only very elementary facts from algebraic geometry [7,section II.6]. We give a proof based on straightforward calculations. A better proof based on class groups will be given in a later version. This is tedious work, since we do not have a global expression for the addition law. We can simplify matters a lot with the following lemma.

(1.5) **Lemma.** Let R_0 be the ring $R_0 = \mathbf{Z}[X_1,Y_1,Z_1,X_2,Y_2,Z_2,A,B] \,/\, (F_1,F_2)$, where
$F_i = Y_i^2Z_i - X_i^3 - AX_iZ_i^2 - BZ_i^3$ for $i = 1, 2$.
Then there exist nine polynomials S_j , T_j , U_j in R_0 , for $j = 1, 2, 3$, such that

(a) Every 2×2 - submatrix of the matrix $\begin{pmatrix} S_1 & T_1 & U_1 \\ S_2 & T_2 & U_2 \\ S_3 & T_3 & U_3 \end{pmatrix}$ has determinant 0.

(b) For any field K of characteristic $\neq 2$ or 3 , any elliptic curve $E = E_{a,b}$ over K , and any pair of points $P = (x_1:y_1:z_1)$ and $Q = (x_2:y_2:z_2)$ on $E(K)$, we have:
$\begin{pmatrix} s_1 & t_1 & u_1 \\ s_2 & t_2 & u_2 \\ s_3 & t_3 & u_3 \end{pmatrix}$ is a non-zero matrix over K ,
and $P + Q = (s_j:t_j:u_j)$ whenever this is a good projective point, i.e. when at least one of the coordinates is non-zero. Here s_j,t_j,u_j denote the images of S_j , T_j , U_j in K under the homomorphism $\varphi : R_0 \to K$ defined by $\varphi(X_1) = x_1$, ... , $\varphi(B) = b$. Note that P , $Q \in E(K)$ implies that φ is well defined.

PROOF: When we take λ as in (5), we can calculate $(x_1/z_1:y_1/z_1:1) + (x_2/z_2:y_2/z_2:1)$ formally using (1.3). Putting

$$(x_2z_1 + x_1z_2)(x_2z_1 - x_1z_2)^2 =$$
$$y_1^2z_1z_2^3 + y_2^2z_1^3z_2 + x_1x_2^2z_1^2z_2 + x_1^2x_2z_1z_2^2 - ax_1z_1^2z_2^3 - ax_2z_1^3z_2^2 - 2bz_1^3z_2^3$$

and clearing denominators we get polynomials

$$s_1 = -h(x_2z_1 - x_1z_2) ,$$
$$t_1 = h(y_2z_1 - y_1z_2) - (x_2y_1 - x_1y_2)(x_2z_1 - x_1z_2)^2 ,$$
$$u_1 = (x_2z_1 - x_1z_2)^3 ,$$

with

$$h = 2(y_1y_2 - bz_1z_2)z_1z_2 - (x_2z_1 + x_1z_2)(x_1x_2 + az_1z_2) .$$

We see that

$$P + Q = (s_1:t_1:u_1) \text{ whenever } x_2z_1 \neq x_1z_2 \text{ or } h(y_2z_1 - y_1z_2) \neq 0 ,$$

i.e. when $O \neq P \neq Q \neq O$. Other values of P and Q will yield $s_1 = t_1 = u_1 = 0$. Taking the expression for λ as in (6) we obtain polynomials s_2,t_2,u_2 with

$$P + Q = (s_2:t_2:u_2) \text{ whenever } y_2z_1 + y_1z_2 \neq 0 \text{ or } g \neq 0$$

for some polynomial g . The former expression is non-zero when P or $Q = O$, but not both, or when $P = Q \neq O$, except when $P = Q = (x:0:1)$. We can see directly from (6) that

$$t_2(x,0,1,x,0,1) = -(3x^2 + a)^3 + (3x^2 + a)(x + x)(0 + 0) - (0\cdot 0 + 2x^3 + b)(0 + 0) .$$

Now $3x^2 + a \neq 0$ for otherwise $3x^3 = -ax = x^3 + b$ and

$$4a^3 + 27b^2 = 4\cdot(-3x^2)^3 + 27\cdot(2x^3)^2 = 0 ,$$

a contradiction. So if $P = Q = (x:0:1)$ then $t_2 \neq 0$ and we must have $g \neq 0$ and $P + Q = (s_2:t_2:u_2)$.The only case not covered yet is $P = Q = O$. Then we have $y_1y_2 \neq 0$, so we can work in the affine part of $\mathbf{P}^2(K)$ defined by $y \neq 0$.

With the same technique as in (1.3), using the identity $z^2 = x^3 + axz^2 + bz^3$, we have

$$\lambda = \frac{z_2 - z_1}{x_2 - x_1} \quad \text{or} \quad \lambda = \frac{x_1^2 + x_1x_2 + x_2^2 + az_1z_2}{1 - a\,(x_1z_1 + x_2z_2) - b(z_1^2 + z_1z_2 + z_2^2)} ,$$

$$\nu = z_1 - \lambda x_1 , \; x_3 = 2\lambda\nu a + 3\lambda^2\nu b - x_1 - x_2 \text{ and } P + Q = (-x_3 : 1 : -(\lambda x_3 + \nu)) ,$$

the second expression being the one we need for $P = Q = O$. In this way we obtain polynomials s_3,t_3,u_3 which will give an expression for $P + Q$, when P and Q are in a neighbourhood of O. The nine polynomials S_j , T_j , U_j thus obtained certainly satisfy condition (b). To prove the first assertion, first note that R_0 is an integral domain: F_i is Eisenstein at Z_i as a polynomial in X_i. We may assume that K is the field of fractions of R_0 , since the polynomials are independent of K. Now $s_1t_2 = s_2t_1$ etc. for any pair P, Q on $E(K)$, and hence $S_1T_2 = S_2T_1$ in R_0. So any 2×2 - subdeterminant of the matrix must be 0.

We now prove the theorem. The non-trivial verifications are the closedness and associativity of the addition. We will work in the field of fractions L_0 of R_0, and use the fact that the matrix in (a) has rank 1 over L_0. None of the polynomials are identically zero, so we have $S_m = H_{mn}S_n , T_m = H_{mn}T_n , U_m = H_{mn}U_n$ for $H_{mn} = S_m/S_n \in L_0^*$. Omitting suffixes, we have to show that

$$T^2U = S^3 + ASU^2 + BU^3 \quad \text{in } R_0 \tag{7}$$

and

$$S(X_1,Y_1,Z_1,S(X_2,\ldots,Z_3),T(X_2,\ldots,Z_3),U(X_2,\ldots,Z_3)) = G\cdot S(S(X_1,\ldots,Z_2),T(X_1,\ldots,Z_2),U(X_1,\ldots,Z_2),X_3,Y_3,Z_3) \tag{8}$$

for some trihomogeneous non-zero element G in the field of fractions L_1 of the ring

$$R_1 = \mathbf{Z}[A,B][X_1,Y_1,Z_1,X_2,Y_2,Z_2,X_3,Y_3,Z_3\ ] / (F_1,F_2,F_3)\ ,$$

and equally for T and U.

The factor G depends on the indices and not on the coordinate S, T or U involved. In fact we only have to show (7) and (8) for one of the j, since the polynomials are bihomogeneous. If (8) holds for index j, we have

$$\begin{aligned} S_k(X_1,Y_1,Z_1,S_l,T_l,U_l) &= H'_{kj}\, H_{lj}{}^{\alpha}\, S_j(X_1,Y_1,Z_1,S_j,T_j,U_j) \\ &= G_{jjjj}\, H'_{kj}\, H_{lj}{}^{\alpha}\, S_j(S_j,T_j,U_j,X_3,Y_3,Z_3) \\ &= G_{jjjj}\, H'_{kj}\, H_{lj}{}^{\alpha}\, H_{jn}{}^{\alpha}\, H'_{jm}\, S_m(S_n,T_n,U_n,X_3,Y_3,Z_3)\ , \end{aligned}$$

where α is the homogeneous degree of S_j for $j = 1,2,3$. We can take

$$G_{klmn} = G_{jjjj}\, H'_{kj}\, H_{lj}{}^{\alpha}\, H_{jn}{}^{\alpha}\, H'_{jm} = G_{jjjj}\, H'_{kj}\, H_{ln}{}^{\alpha}\, H'_{jm}\ ,$$

with

$$\begin{aligned} H'_{kj} &= H_{kj}(X_1,Y_1,Z_1,S_l,T_l,U_l)\ , \\ H'_{jm} &= H_{im}(S_n,T_n,U_n,X_3,Y_3,Z_3)\ . \end{aligned}$$

For the same reason it is sufficient to show (7) for only one index j as well. The actual calculations can be done by an ambitious bookkeeper or any computer handling formal expressions.

§2. Elliptic curves over rings.

All rings are commutative with 1 and ring homomorphisms are unitary.

(2.1) **Definition.** Let R be a ring. A collection $(a_i)_{i \in I}$ of elements of R is *primitive* if it generates the unit ideal, i.e. there exist $b_i \in R$, almost all zero, such that $\sum_{i \in I} b_i a_i = 1$.

This terminology will in particular be applied to vectors and matrices over R. Note that if R is a field, a collection $(a_i)_{i \in I}$ is primitive if and only if not all a_i are zero. We will consider rings that satisfy the following conditions:

(2.2) $6 = 1 + 1 + 1 + 1 + 1 + 1 \in R^*$.

(2.3) For every pair of integers n, m and every primitive $n \times m$ - matrix over R with the property that every 2×2 - subdeterminant is 0, there exists a linear combination of the rows that is a primitive vector in R^m.

The first condition is by no means essential. It allows us to use the simple form of the equation for an elliptic curve. If we have a homomorphism $R \to K$ then char $K \neq 2$ or 3, so we can consider elliptic curves over K in the sense of (1.1). The second condition however is indispensable for our definition of elliptic curves over rings and their addition law. Examples of rings that satisfy (2.3) are among others fields and finite rings, as we shall see.

(2.4) **Proposition.** The primitive linear combination in (2.3) is unique up to multiplication by units of R.

PROOF: Let (a_{ij}) be the matrix and put $a_1 = (a_{11},...,a_{1m})$,..., $a_n = (a_{n1},...,a_{nm})$. For a primitive linear combination $b = \sum_l \lambda_l a_l = (b_1,...,b_m)$ we have

$$b_j a_{ik} - b_k a_{ij} = \sum_l \lambda_l a_{lj} a_{ik} - \sum_l \lambda_l a_{lk} a_{ij} = 0 \text{ for } 1 \le i \le n \text{ and } 1 \le j,k \le m,$$

since every 2×2 - subdeterminant of the matrix vanishes. Hence $b_j a_i = b a_{ij}$ for $1 \le i \le n$ and $1 \le j \le m$.. There exist $\mu_j \in R$ such that $\sum_j \mu_j b_j = 1$ so we see that

$$a_i = \sum_j \mu_j b_j a_i = \sum_j \mu_j a_{ij} b \in Rb .$$

This shows that $\sum Ra_i \subset Rb$. Since clearly $Rb \subset \sum Ra_i$, all primitive linear combinations generate the same R-module. Let c be another primitive linear combination and let $r, s \in R$ such that $b = rc$ and $c = sb$. Then $rsb_j = b_j$ for all j, so $0 = \sum_j \mu_j b_j (rs - 1) = rs - 1$ and $r, s \in R^*$.

(2.5) **Definition.** Let R be a ring satisfying (2.3) and n a positive integer. The n-dimensional projective space over R, denoted $\mathbf{P}^n(R)$, is the set of primitive $n+1$ - tuples of R, modulo the

equivalence relation $(a_0,\ldots,a_n) \sim (b_0,\ldots,b_n)$ if there exists $u \in R^*$ with $a_i = ub_i$. The equivalence class of $(a_0,\ldots,a_n)$ is denoted by $(a_0{:}\ldots{:}a_n)$.

(2.6) **Definition.** Let R be a ring satisfying (2.3) and (2.4). An *elliptic curve* $E = E_{a,b}$ over R is a pair $(a,b) \in R \times R$ such that $4a^3 + 27b^2 \in R^*$. An *isomorphism* $E \to E'$ is an element $u \in R^*$ with $a' = u^4a$ and $b' = u^6b$. The *set of points* of an elliptic curve is

$$E(R) = \{\ (x{:}y{:}z) \in \mathbf{P}^2(R) \mid y^2z = x^3 + axz^2 + bz^3\ \}$$

Note that $(0{:}1{:}0)$ is in general not the only point on $E(R)$ with $z = 0$. In fact, if $(x{:}y{:}0) \in E(R)$ then $x^3 = 0$ and since a nilpotent element is contained in every maximal ideal of R, the second coordinate y must be a unit. So the points at infinity are $(x{:}1{:}0)$ with $x^3 = 0$.

Let $E = E_{a,b}$ be an elliptic curve over R, and $P = (x_1{:}y_1{:}z_1)$ and $Q = (x_2{:}y_2{:}z_2)$ two points on $E(R)$. We are going to define the sum of P and Q. If R_0 is the ring defined in (1.5) there is a canonical homomorphism $R_0 \to R$ sending X_1 to x_1 etc. The image of the matrix in (1.5) is primitive. For suppose it were not, then all its coordinates would be contained in some maximal ideal $\underline{m}$ of R. The field $K = R/\underline{m}$ has characteristic $\neq 2$ or 3, so $E_{a \bmod \underline{m}, b \bmod \underline{m}}$ defines an elliptic curve over K, and P and Q are good projective points over K, since their coordinates form a primitive vector in R^3. Hence $\overline{P} + \overline{Q} = (\overline{s}_i{:}\overline{t}_i{:}\overline{u}_i) \neq (0{:}0{:}0)$ for some i, which is a contradiction. Since R satisfies (2.3) there exists a primitive linear combination (s_4,t_4,u_4) of the rows which is unique up to multiplication by units.

(2.7) **Theorem.** $E(R)$ has a natural abelian group structure, with zero-element $O = (0{:}1{:}0)$, inverse $-(x{:}y{:}z) = (x{:}-y{:}z)$ and $(x_1{:}y_1{:}z_1) + (x_2{:}y_2{:}z_2) = (s_4{:}t_4{:}u_4)$ as defined above.

PROOF: In the case that R is a field, $(s_i{:}t_i{:}u_i) = (s_4{:}t_4{:}u_4)$ for some i, and $t_4^2u_4 - s_4^3 - as_4u_4^2 - bu_4^3 = 0$, by lemma (1.5). This goes for any field, so putting $(s_4,t_4,u_4) = \sum \lambda_i(s_i,t_i,u_i)$, it follows that $T_4^2U_4 - S_4^3 - AS_4U_4^2 - BU_4^3 = 0$ in $R_0[\Lambda_1,\Lambda_2,\Lambda_3]$ and consequently $E(R)$ is closed under addition for all rings R. It is clear from the identities in the proof of (1.4) that the addition satisfies the other group axioms.

Since a finite ring is a product of local rings (i.e. rings with a unique maximal ideal), it is clear by exercise (2.1) that finite rings satisfy (2.3). However, we will give a "constructive" proof of this, which will give us a method to compute the primitive linear combination, provided we have algorithms to add, multiply and solve linear equations in the ring. Note that in $\mathbf{Z}/n\mathbf{Z}$ we can solve linear equations using the Euclidean algorithm. We need a lemma first.

(2.8) **Lemma.** Let R be a finite ring and $c \in R$. Then there exist $x \in R$ and $t \in \mathbf{Z}_{\geq 0}$, with $t \leq \log \#R / \log 2$, such that $c^t = c^{t+1} \cdot x$.

PROOF: Consider the sequence $R \supseteq Rc \supseteq Rc^2 \supseteq \ldots$. Since R is finite this sequence must stop, which proves the existence of t and x. Furthermore the smallest such t satisfies $2^t \leq [R:Rc^t] \leq \#R$.

Now let $R \neq \{0\}$ be a finite ring and $A = (a_{ij})$ a matrix over R as in (2.3). Choose an element c from (a_{ij}) which is not nilpotent. If $c \in R^*$ the row containing c is primitive and we're done. Otherwise calculate $t > 0$ and x such that $c^t = c^{t+1}x$. Since $c^t = cc^tx = \ldots = c^{2t}x^t$, the element $e = x^tc^t$ is an idempotent, i.e. $e^2 = e$ and $e(1-e) = 0$. By the Chinese remainder theorem we have a decomposition $R \cong R/Re \times R/R(1-e)$. Since e is neither zero nor a unit the orders of these two rings are strictly smaller than the order of R and the result follows by induction.

Note that we actually have $R \cong R(1-e) \times Re = R_1 \times R_2$, where $1-e$ and e are the unit elements of R_1 and R_2 respectively. Under this isomorphism an element r is mapped to $((1-e)r,er)$. Now ec is a unit in R_2, with inverse $ec^{t-1}x^t$, so we only have to apply the recursion in one direction. Moreover $c - ec$ is nilpotent in R_1, so the number of nilpotent elements in the matrix A_1 over R_1, induced by the matrix A, is at least one more than in A itself. Hence the recursion depth is bounded by mn, if A is an $n \times m$ - matrix. The fact that the ring operations in R_1 and R_2 are the same as in R will also be very convenient in applications.

When the induction is carried out completely, we see that R factors into a product of rings in which every element is either a unit or nilpotent. Since all such rings are local, we have proved that a finite ring is the product of local rings.

Exercises.

2.1 Show that the following rings satisfy (2.3):
- (a) fields;
- (b) semi-local rings (i.e. rings that contain only finitely many maximal ideals);
- (c) finite products of rings that satisfy (2.3);
- (d) principal ideal domains.

2.2 Let R be a ring and A an $n \times m$ - matrix as in (2.3). Let $M = \sum Ra_i \subseteq R^m$, where a_i is the i^{th} m - dimensional row vector of the matrix.
- (a) Prove that there is a module $N \subseteq R^m$ with $M \oplus N = R^m$. (Hence M is a finitely generated projective R - module.)

(b) Prove that M has constant rank 1, i.e. $\dim_{R/\underline{m}}(M/\underline{m}M) = 1$ for all maximal ideals $\underline{m}$ of R.

(c) Show that any module satifying (a) and (b) is in fact a module such as M.

2.3 Show that the following statements are equivalent:

(a) R satisfies (2.3);

(b) Pic $R = 0$;

(c) Every projective R - module of rank 1 is free.

Here the *Picard group* Pic R is the group of isomorphism-classes of invertible R-modules, with multiplication given by $\langle M\rangle\langle N\rangle = \langle M \otimes N\rangle$, $1 = \langle R\rangle$, $\langle M\rangle^{-1} = \langle \mathrm{Hom}_R(M,R)\rangle$.

2.4 Show that if R is a Dedekind domain, R satisfies (2.3) if and only if R is a principal ideal domain.

2.5 Show that the matrix $\begin{pmatrix} S_1 & T_1 & U_1 \\ S_2 & T_2 & U_2 \\ S_3 & T_3 & U_3 \end{pmatrix}$ is primitive over $R_0[1/6,(4A^3 + 27B^2)^{-1}]$.

2.6 Let R, R' be two rings satisfying (2.2) and (2.3), and $f: R \to R'$ a ring homomorphism. If $E = E_{a,b}$ is an elliptic curve over R , then $E_{f(a),f(b)}$ is an elliptic curve over R', and f induces a group homomorphism $f_* : E(R) \to E(R')$.

(a) If f is injective then so is f_* .

(b) If R is a principal ideal domain and R' is its field of fractions, then f_* is an isomorphism.

2.7 Let R be a ring satisfying (2.2) and (2.3) and $\underline{a} \subseteq R$ a nilpotent ideal, i.e. $\underline{a}^n = 0$ for some n. Suppose E is an elliptic curve over R. Show that:

*(a) $f_* : E(R) \to E(R/\underline{a})$ is surjective.

(b) $\ker(f_*) = \{ (x:1:z) \in E(R) \mid x,z \in \underline{a} \}$.

(c) The map $\ker(f_*) \to \underline{a}$, defined by $(x:1:z) \mapsto x$ is bijective.

(d) The composed map $\ker(f_*) \to \underline{a} \to \underline{a}/\underline{a}^5$ is a group homomorphism.

2.8 Let E be an elliptic curve over a field K and $f: K[[T]] \to K[[T]]/T\cdot K[[T]] \cong K$ the canonical homomorphism of the ring of formal power series over K onto K. Denote $H = \ker(f_*)$ and $\underline{a} = TK[[T]]$.

(a) Show that $H = \{ (x:1:z) \in E(K[[T]]) \mid x,z \in \underline{a} \}$.

(b) Show that $H \to \underline{a}$, $(x:1:z) \mapsto x$ is a bijection and the composed map $H \to \underline{a}/\underline{a}^5$ is a group homomorphism.

§3. The j - invariant.

Let K be a field of characteristic $\neq 2$ or 3. We have seen that $E_{a,b} \cong E_{u^4a,u^6b}$,where $u \in K^*$. Hence we can attach an invariant $(a^3:b^2) \in \mathbf{P}^1(K)$ to the elliptic curve $E_{a,b}$. Given the bijection $\mathbf{P}^1(K)$-$\{(27:-4)\} \to K$, sending $(x:y)$ to $4x/(4x + 27y)$, we can define the j - invariant.

(3.1) **Definition.** The j - *invariant* of an elliptic curve $E = E_{a,b}$ is

$$j(E) = 1728 \cdot \frac{4a^3}{4a^3 + 27b^2} \in K .$$

The normalization by the factor $1728 = 12^3$ stems from the fact that this formula is derived from the general formula for fields of arbitrary characteristic. We have seen that two isomorphic elliptic curves have the same j - invariant. The converse is not true for general fields (see exercise 3.1), but we do have the following theorem. We denote by $\overline{K}$ the algebraic closure of K.

(3.2) **Theorem.**
(a) The map $j : \{E : \text{elliptic curve over } K\}/\cong_K \to K$ is surjective.
(b) $j(E) = j(E') \Leftrightarrow E \cong_{\overline{K}} E'$ (hence j is bijective if $K = \overline{K}$).

PROOF: (a) First of all $j(E_{a,b}) = 0 \Leftrightarrow a = 0$ and $j(E_{a,b}) = 1728 \Leftrightarrow b = 0$. For $c \in K$-$\{0,1728\}$ we have $j(E_{a,a}) = c$ with $a = {}^{27}/_{4} \cdot {}^{c}/_{1728-c}$, or $j(E_{3a,2a}) = c$ with $a = {}^{c}/_{1728-c}$.
(b) If $j(E_{a,b}) = j(E_{a',b'}) = 0$ then $a = a' = 0$. Since $\overline{K}$ is algebraically closed, there exists $u \in \overline{K}^*$ such that $b = u^6 b'$, so $E \cong E'$. Similarly we deal with $j = 1728$. In other cases $a,b,a',b' \neq 0$, and an element $u \in \overline{K}^*$ satisfying $u^2 = {}^{b/b'}/_{a/a'}$ is an isomorphism $E \to E'$.

Exercises.

3.1 Show that for every $j \in \mathbf{Q}$ there exist infinitely many pairwise non-isomorphic elliptic curves $E/\mathbf{Q}$ with $j(E) = j$.

3.2 Let $K = \mathbf{F}_q$ be a finite field of characteristic $\neq 2$ or 3 and let E/K be an elliptic curve.

(a) Prove that $\#\{ E'/K \mid j(E') = j(E) \}/\cong_K = \#\mathrm{Aut}_K(E) = \begin{cases} 6 \text{ if } q \equiv 1 \pmod 6 \text{ and } j = 0 \\ 4 \text{ if } q \equiv 1 \pmod 4 \text{ and } j = 1728 \\ 2 \text{ otherwise} \end{cases}$

(b) Describe all a',b' with $j(E_{a,b}) = j(E_{a',b'})$.

(c) Let $C = \{E : \text{elliptic curve over } K\}/\cong_K$. Show that $\#C = 2q + \begin{cases} 6 \text{ if } q \equiv 1 \pmod{12} \\ 4 \text{ if } q \equiv 7 \pmod{12} \\ 2 \text{ if } q \equiv 5 \pmod{12} \\ 0 \text{ if } q \equiv 11 \pmod{12} \end{cases}$

(d) Show that $\sum_{E \in C} (\#\mathrm{Aut}_K(E))^{-1} = q$.

§4. Morphisms and isogenies.

Throughout this section K will be a field of characteristic $\neq 2$ or 3. Elements $f \in K(X)$ are written $f = f_1/f_2$, with $f_i \in K[X]$ coprime and f_2 monic. Furthermore E will be the elliptic curve $E = E_{a,b}$ and $F = X^3 + aX + b$.

(4.1) **Definition.** Let E be an elliptic curve over K. The *coordinate ring* of E/K is the ring $K[E] = K[X,Y]/(Y^2 - F) \cong K[X, \sqrt{F}]$. The *function field* of E is the field of fractions of $K[E]$, denoted $K(E) \cong K(X, \sqrt{F})$.

(4.2) **Definition.** Let E and E' be elliptic curves over K. A *morphism* $\varphi : E \to E'$ over K is an element φ of $E'(K(E))$ that is either equal to O, or of the form

$$\varphi = (f : g\sqrt{F} : 1) \text{ , with } f,g \in K[X] \text{ and } \deg f_1 > \deg f_2.$$

An *isogeny* is a morphism that is not equal to O. The *degree* of a morphism is

$$\deg \varphi = \begin{cases} 0 \text{ if } \varphi = O, \\ \deg f_1 \text{ if } \varphi = (f : g\sqrt{F} : 1). \end{cases}$$

If $\varphi : E \to E'$ is a morphism and $L \supset K$ a field extension of K, then φ induces a map from the set of points $E(L)$ to the set of points $E'(L)$. We shall denote this map by abuse of notaion by the same symbol φ. Explicitly this map is defined by $\varphi(P) = O$ if $\varphi = O$ and if $\varphi = (f : g\sqrt{F} : 1)$ then

$$\varphi(O) = O$$

and

$$\varphi((x:y:1)) = \begin{cases} O \text{ if } f_2(x) = 0, \\ (f(x) : g(x)y : 1) \text{ if } f_2(x) \neq 0. \end{cases}$$

This is a well defined map (see exercise (4.1)).

An isogeny $\varphi = (f : g\sqrt{F} : 1)$ induces a homomorphism of fields $\varphi^* : K(E') \to K(E)$, defined by $X \mapsto f$, $\sqrt{F'} \mapsto g\sqrt{F}$. This homomorphism is injective and $K(E)$ is a finite field extension of $\varphi^* K(E')$.

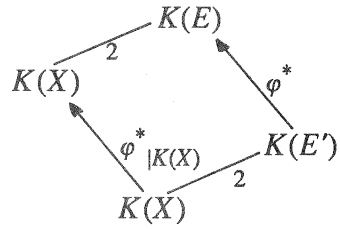
(4.3) **Example.** The *identity morphism* $[1] = 1_E = 1 = \mathrm{id}_E : E \to E$ is the morphism $[1] = (X : \sqrt{F} : 1)$. This is an isogeny of degree 1. We shall see in the next section that for every $m \in \mathbf{Z}$ there is a morphism $[m] : E \to E$, called the *multiplication-by-m* map, which maps $P \in E(L)$ to $mP = \pm(P + \ldots + P)$ ($|m|$ times). This is a morphism of degree m^2. See also exercise (4.4).

(4.4) **Example.** Let K be a field of characteristic $p \geq 5$ and let q be a power of p. The

Frobenius morphism $\mathrm{Frob}_q : E = E_{a,b} \to E_{a^q,b^q} = E^{(q)}$ is the element $(X^q : (\sqrt{F})^q : 1) = (X^q : F^{(q-1)/2}\sqrt{F} : 1)$ of $E^{(q)}(K(E))$. This is an isogeny of degree q.

(4.5) **Theorem.** If φ is an isogeny then $[K(E) : \varphi^* K(E')] = \deg \varphi$.

PROOF: We have the following diagram of field extensions:



From this diagram it is clear that

$$[K(E) : \varphi^* K(E')] = [K(X) : \varphi^* K(X)] = [K(X) : K(f)] .$$

We claim that the minimum polynomial of X over $K(f)$ is $M = f_1(T) - f f_2(T) \in K(f)[T]$. Since $\deg f_1 > \deg f_2$, this shows that

$$[K(X) : K(f)] = \deg M = \deg f_1 = \deg \varphi .$$

To prove the claim it is sufficient to show that M is irreducible. Note that M is primitive as a polynomial in $K[f][T]$ since its leading coefficient is a unit. By the lemma of Gauss M is irreducible in $K(f)[T]$ if and only if it is irreducible in $K[f][T] = K[T][f]$. Now $\deg f_1 > 0$, so f is a transcendental variable over $K(T)$. Since f_1 and f_2 are coprime we can apply Gauss' lemma again, hence we have to show that M is irreducible in $K(T)[f]$. This is evidently true, since M has degree 1 as a polynomial in f.

(4.6) **Theorem.** Let $\varphi : E \to E'$ be a morphism and $L \supset K$ a field extension of K. Then the induced map $\varphi : E(L) \to E'(L)$ is a group homomorphism.

An elementary proof of this theorem will be included in one of the following versions. The reader who is familiar with function fields and divisor classes can find a proof in Silverman [19, section III.4]. It can be verified easily that all morphisms we will consider, except the ones in exercise (4.3), satisfy the statement of the theorem.

Of course we would like that morphisms have categorical properties. If two morphisms $\varphi : E \to E'$ and $\varphi' : E' \to E''$ are both not O, the composition of their induced maps $E(L) \to E'(L) \to E''(L)$ takes almost all elements $(x:y:1)$ to $(f'(f(x)) : g'(f(x))g(x)y : 1)$.

(4.7) **Definition.** Let $\varphi : E \to E'$ and $\varphi' : E' \to E''$ be two morphisms. The composition φ''

$= \varphi' \circ \varphi \in E''(K(E))$. is defined as:

$$\varphi'' = \begin{cases} O \text{ if } \varphi = O \text{ or } \varphi' = O, \\ (f' \circ f : (g' \circ f) \cdot g\sqrt{F} : 1) \text{ otherwise.} \end{cases}$$

If φ and φ' are isogenies they induce field homomorphisms over K

$$\begin{array}{rcl} \varphi'^* : K(X, \sqrt{F''}) & \to & K(X, \sqrt{F'}) \\ X & \mapsto & f'(X) \\ \sqrt{F''} & \mapsto & g'(X)\sqrt{F'} \end{array} \qquad \text{and} \qquad \begin{array}{rcl} \varphi^* : K(X, \sqrt{F'}) & \to & K(X, \sqrt{F}) \\ X & \mapsto & f(X) \\ \sqrt{F'} & \mapsto & g(X)\sqrt{F} \end{array},$$

hence $\varphi^* \circ \varphi'^* : K(E'') \to K(E)$ is given by $X \to f'(f(X))$ and $\sqrt{F''} \to g'(f(X))g(X)\sqrt{F}$. This shows that $\varphi''^* = \varphi^* \circ \varphi'^*$, giving a tower of field extensions $K(E'') \subset K(E') \subset K(E)$ and so $\deg \varphi'' = \deg \varphi \cdot \deg \varphi'$. We leave it to the reader to check that φ'' is indeed a morphism, and that the induced map of φ'' is the composition of the induced maps of φ and φ'.

The degree of an isogeny can be interpreted in another way than being a property of the function fields. For general curves and finite morphisms instead of isogenies the degree of a morphism is the number of points in a "typical" fibre. When K is an algebraically closed field all fibres have the same number of points, if counted with the right multiplicity. For general fields this is no longer true. In the case of elliptic curves and isogenies the situation is quite simple, due to the fact that isogenies are homomorphisms: all fibres have the same number of points and therefore all points in a fibre have the same multiplicity. When the isogeny is separable and K is algebraically closed this multiplicity is equal to 1. Before specifying what is meant by a separable isogeny we recall some facts from algebra.

(4.8) **Definition.** Let K be a field. A polynomial $f \in K[X]$ is called *separable* if f has no double roots in the algebraic closure of K.

(4.9) **Theorem.** Let K be a field and $f \in K[X]$ a polynomial with derivative f'. Then f is separable if and only if $\gcd(f,f') = 1$ in the ring $K[X]$.

PROOF: If f is separable and $g \mid f,f'$ then every zero of g is a double zero of f, hence g must be a unit. Conversely, if $\gcd(f,f') = 1$ then there exist g_1 and g_2 such that $fg_1 + f'g_2 = 1$, so f and f' have no roots in common.

(4.10) **Theorem.** If f is irreducible in $K[X]$ then f is separable if and only if $f' \neq 0$.

PROOF: Since $\deg f' < \deg f$ we must have $\gcd(f,f') = 1$ if f is irreducible and $f' \neq 0$. If on the

contrary $f' = 0$, and $f = \sum a_i X^i$, then necessarily $ia_i = 0$ for all i. This is impossible if char $K = 0$, and if char $K = p > 0$ it follows that $f \in K[X^p] \subset (\overline{K}[X])^p$ and we see that f has p-tuple roots.

Hence for irreducible polynomials inseparability is easy to check. A typical example of an inseparable polynomial is $X^p - a$, if a is not a p^{th} power in a field of characteristic $p > 0$. We are now ready to define separable and inseparable morphisms.

(4.11) **Definition.** An isogeny $\varphi = (f : g\sqrt{F} : 1)$ is called *inseparable* if char $K = p > 3$ and $f \in K(X^p)$, and otherwise *separable*. The morphism O is also called inseparable.

In the next section we shall give a geometric characterization of (in)separability in terms of actions on tangent spaces.

(4.12) **Proposition.** Let $\varphi = (f:g\sqrt{F}:1)$ be an isogeny $E \to E'$, defined over a field K of characteristic $p > 0$. Then the following are equivalent:

(a) φ is inseparable ;

(b) $f_1, f_2 \in K[X^p]$;

(c) $f_1 - Tf_2 \in K(T)[X]$ is inseparable as a polynomial over $K(T)$;

(d) There is an isogeny $\psi : E^{(p)} \to E'$ with $\varphi = \psi \circ \text{Frob}_p$;

(e) $\varphi \in E'(K(X^p,(\sqrt{F})^p))$.

PROOF: We prove a $\Rightarrow$ b $\Rightarrow$ e $\Rightarrow$ d $\Rightarrow$ a and b $\Leftrightarrow$ c.

(a$\Rightarrow$b) Since $f \in K(X^p)$ we can write $f = h_1(X^p) / h_2(X^p)$ with $\gcd(h_1,h_2) = 1$, h_2 monic. It is sufficient to show that $\gcd(h_1(X^p),h_2(X^p)) = 1$ for in that case $f_i = h_i(X^p)$. We can show this by substituting X^p for X in the expression $u_1h_1 + u_2h_2 = 1$.

(b$\Leftrightarrow$c) This is trivial since $f_1 - Tf_2$ is irreducible in $K(T)[X]$. (See proof of (4.5).)

(b$\Rightarrow$e) If $g = 0$ then obviously $\varphi \in E'(K(X^p,(\sqrt{F})^p))$. Otherwise $g^p \in K(X^p)$ since char $K = p$ and $(g\sqrt{F})^2 = f^3 + a'f + b' \in K(X^p)$ since $f \in K(X^p)$ and therefore, putting $p = 2q+1$, we see that $g\sqrt{F} = (g^p / (g\sqrt{F})^{2q}) \cdot (\sqrt{F})^p \in K(X^p,(\sqrt{F})^p)$.

(e$\Rightarrow$d) We can write $K(X^p,(\sqrt{F})^p) = K(X^p) \oplus (\sqrt{F})^pK(X^p)$. Since by definition $f,g \in K(X)$ we must have $f = f'(X^p)$ and $g\sqrt{F} = g'(X^p)\cdot(\sqrt{F})^p$, with $f',g' \in K(X)$. Hence $\psi = (f':g'\sqrt{F'}:1)$ will do, where $F' = X^3 + a^pX + b^p$.

(d$\Rightarrow$a) If $\psi = (f':g'\sqrt{F'}:1)$ then $\psi \circ \text{Frob}_p = (f'(X^p) : g'(X^p)\cdot(\sqrt{F})^p : 1)$, so φ is inseparable.

(4.13) **Corollary.** Every isogeny φ has a unique decomposition $\varphi = \varphi_{\text{sep}} \circ \text{Frob}_q$, with φ_{sep} separable and $q = p^n$ for some $n \geq 0$. (We take $q = 1$ if $p = 0$.)

Remark: We call $q = \deg_i \varphi$ the *inseparable degree* of φ and $\deg \varphi_{\text{sep}} = \deg_s \varphi$ the *separable degree* of φ.

PROOF: If φ is separable we take $q = 1$. If φ is inseparable we can write $\varphi = \psi \circ \text{Frob}_p$ by (4.12.d) and the result follows by induction since $\deg \psi < \deg \varphi$. Note that $\text{Frob}_q \circ \text{Frob}_{q'} = \text{Frob}_{q \cdot q'}$. Verifying the uniqueness is left to the reader.

The reader who is familiar with the theory of field extensions will not be surprised to see that $\deg_i(\varphi) = [K(E'):\varphi^* K(E)]_i$ and $\deg_s(\varphi) = [K(E'):\varphi^* K(E)]_s$, the inseparable and separable degree of the field extension $K(E') / \varphi^* K(E)$. Corollary (4.13) is analogous to the field theoretic situation where a finite field extension $L \supset K$ factorizes into $L \supset M \supset K$ where M/K is a separable extension and L/M is a purely inseparable extension, i.e. $\alpha^q \in M$ for every $\alpha \in L$.

(4.14) **Theorem.** Let $\varphi : E \to E'$ be an isogeny over K. Let $L \supset K$ be an algebraically closed field. Then the induced map $\varphi : E(L) \to E'(L)$ is surjective and $\#\ker \varphi = \deg_s \varphi$.

PROOF: Note that $\text{Frob}_p : E(L) \to E^{(p)}(L)$ is bijective if $\text{char } K = p$. We may therefore assume by corollary (4.13) that $\varphi = (f:g\sqrt{F}:1)$ is separable. In this case $h = f_1 - Tf_2 \in K(T)[X]$ is separable as a polynomial over $K(T)$. Hence by theorem (4.7) there exist $\lambda, \mu \in L[T,X]$ and $\nu \in L[T]$, $\nu \neq 0$, with $\lambda h + \mu h' = \nu$. Choose $t \in L$ such that $\nu(t) \neq 0$ and $F(t) \neq 0$. Then $h_t = f_1 - tf_2$ is separable as a polynomial over $L[X]$ and so

$$\#\{ x \in L \mid h_t(x) = 0 \} = \deg h_t = \deg f_1 = \deg \varphi = \deg_s \varphi .$$

Let $P = (t:u:1) \in E'(L)$. If $h_t(x) = 0$ and $Q = (x:y:1) \in E(L)$ then $\varphi(Q) = \pm P$ and necessarily $\varphi(\pm Q) = P$ since φ is a group homomorphism. Now $F(t) \neq 0$ so $P \neq -P$ and the conclusion is that for every root x of h_t there exists exactly one point $Q = (x:y:1)$ with $\varphi(Q) = P$. So

$$\#\varphi^{-1}(P) = \deg_s \varphi \text{ for all but finitely many points on } E'(L).$$

(Namely all affine points (t,u) with $\nu(t) \cdot F(t) \neq 0$.) We see first of all that the subgroup $\varphi[E(L)]$ of $E'(L)$ has a finite complement and since $E'(L)$ is infinite this complement must be empty, whence φ is surjective. Secondly

$$\#\ker \varphi = \text{the number of points in the fibre of an arbitrary point} = \deg_s \varphi .$$

Exercises.

4.1 (a) Check that the map $E(L) \to E'(L)$ induced by the morphism $\varphi : E \to E'$ is well defined. Show in particular that $g_2(x) \neq 0$ if $f_2(x) \neq 0$.

(b) Show that the Frobenius-morphism and the multiplication-by-m map are group

homomorphisms.

4.2 (a) Show that every isogeny of degree 1 with domain E is of the form $(u^2X:u^3\sqrt{F}:1)$ with $u \in K^*$, and conversely such an element of $E'(K(E))$,where $E' = E_{u^4a,u^6b}$, is indeed an isogeny of degree 1. Hence there is a one to one correspondence between isogenies of degree 1 and isomorphisms as defined in (1.2).

(b) An isogeny of degree 1 induces a group isomorphism. Give an example to show that the converse is not true (not even in characteristic 0).

4.3 (a) Show that $(\dfrac{X^2+a}{X} : \dfrac{X^2-a}{X^2}\sqrt{F} : 1)$ is an isogeny $E_{a,0} \to E_{-4a,0}$ of degree 2.

(b) Show that $E_{a,0} \cong E_{-4a,0}$ if and only if $i \in K^*$, i.e. -1 is a square in K^*.

(c) Show that $(\dfrac{X^3+4b}{X^2} : \dfrac{X^3-8b}{X^3}\sqrt{F} : 1)$ is an isogeny $E_{0,b} \to E_{0,-27b}$ of degree 3.

(d) Show that $E_{0,b} \cong E_{0,-27b}$ if and only if $\zeta_3 \in K^*$, i.e. -3 is a square in K^*.

(e) Show that if $K = \mathbf{R}$ and $b < 0$ the isogeny in (c) induces a bijection.

4.4 (a) Using formula (6) from section 1, show that if $P = (x,y) \in E(K)$, with $y \neq 0$, then

$$P + P = (f(x):g(x)y:1) ,$$

with

$$f = \frac{(F')^2 - 8X\cdot F}{4F} \quad , \quad g = \frac{12X\cdot F\cdot F' - (F')^3 - 8F^2}{8F^2} \in K(X) .$$

(Here F' denotes the derivative of $F = X^3 + aX + b$.)

(b) Show that $(f : g\sqrt{F} : 1) \in E(K(E))$ is an isogeny.

(c) Conclude that the multiplication-by-2^n-map $[2^n] : E \to E$ is an isogeny of degree 2^{2n}.

§5. Addition of morphisms.

The set of morphisms $E \to E'$ is a subset of the abelian group $E'(K(E))$. At first sight it is not clear that the sum of two morphisms is a morphism, nor that $(\varphi + \psi)(P) = \varphi(P) + \psi(P)$. In this section we will see that both statements are true. Before doing so we embed the function field $K(E)$ into the field of formal Laurent series over K.

(5.1) **Definition.** The field of *formal Laurent series* over K is

$$K((t)) = \{ \sum_{i \geq n} a_i t^i \mid n \in \mathbf{Z}, a_i \in K \},$$

with the evident addition and multiplication. The *degree* of a formal Laurent series $f = \sum_{i \geq n} a_i t^i \neq 0$ is $\deg f = \min\{i \in \mathbf{Z} \mid a_i \neq 0\}$. The degree function is a group homomorphism from the multiplicative group $K((t))^*$ to the additive group $\mathbf{Z}$.

(5.2) **Proposition.** Let E be an elliptic curve. For every point $P \in E(K)$ there is a K-homomorphism $i_P : K(E) \to K((t))$, defined as follows:

If $P = O$ then $\begin{cases} X \mapsto t^{-2} \\ \sqrt{F} \mapsto \alpha = t^{-3} + \text{h.o.t.} \quad \text{such that } \alpha^2 = F(t^{-2}) \end{cases}$

If $P = (x{:}y{:}1)$ and $y \neq 0$ then $\begin{cases} X \mapsto x + t \\ \sqrt{F} \mapsto \alpha = y + \text{h.o.t.} \quad \text{such that } \alpha^2 = F(x + t) \end{cases}$

If $P = (x{:}y{:}1)$ and $y = 0$ then $\begin{cases} X \mapsto x + t^2/F'(x) \\ \sqrt{F} \mapsto \alpha = t + \text{h.o.t.} \quad \text{such that } \alpha^2 = F(x + t^2/F'(x)) \end{cases}$

(h.o.t. = higher order terms.)

PROOF: The only thing to be proved is the existence of α. This can be done in many ways. One could approximate the solution recursively by solving $(a_0 + \ldots + a_n t^n)^2 \equiv f \pmod{t^{n+1}}$ for successive n, where

$$\begin{aligned} f &= t^6 F(t^{-2}) = 1 + at^4 + bt^6, \\ f &= F(x + t) = y^2 + F'(x)t + 3xt^2 + t^3 \quad \text{or} \\ f &= t^{-2} F(x + t^2/F'(x)) = t^{-2}(x^3 + ax + b + t^2 + 3xF'(x)^{-2}t^4 + F'(x)^{-3}t^6) \\ &= 1 + 3xF'(x)^{-2}t^2 + F'(x)^{-3}t^3 \quad \text{respectively.} \end{aligned}$$

When worked out one sees that this is always possible since $(f \bmod t) \in K$ is a non-vanishing square, and that the leading coefficient a_0 of $\sqrt{f}$ is a square root of $(f \bmod t)$. This can be seen directly using Hensel's lemma, of which the last remark is just a special instance.

If all else fails one could use Newton's formula $(1 + u)^{1/2} = \sum_{j \geq 0} \binom{1/2}{j} u^j$.

The embeddings i_P allow us to consider an element f of the function field $K(E)$ really as a (rational) function $f: E(K) \to \mathbf{P}^1(K) = K \cup \{\infty\}$. The value of f is defined as

$$f(P) = i_P(f)(0)$$

with the convention that $i_P(f)(0) = \infty$ if $\deg i_P(f) < 0$.

The representation of a function as a formal Laurent series contains all the local information of the function around a point. This is completely analoguous to representing a meromorphic function in complex analysis as a Laurent series around a point P which is convergent in a (reduced) neighbourhood of P.

Let E' be another elliptic curve over K. Since $K[[t]]$ is a principal ideal domain the map $i_P: K(E) \to K((t))$ induces by exercise (2.6) an injective group homomorphism $(i_P)_*: E'(K(E)) \to E'(K[[t]])$. Furthermore the canonical map $K[[t]] \to K$, $t \mapsto 0$, induces a group homomorphism $h: E'(K[[t]]) \to E'(K)$.

(5.3) **Definition.** Let E,E' be two elliptic curves. The *evaluation map* $h_P: E'(K(E)) \to E'(K)$ is the composed map $h_P = h \circ (i_P)_*$.

In exercise (5.1) it is shown that if $f,g,h \in K(E)$ then $h_P(f:g:h) = (f(P):g(P):h(P))$ provided all negative powers of t in the Laurent series are multiplied out. In particular $h_P(\varphi) = \varphi(P)$ for morphisms φ.

(5.4) **Theorem.** The set of morphisms $\mathrm{Hom}_K(E,E')$ is a subgroup of $E'(K(E))$ and is contained in the kernel of h_O.

PROOF: The proof is divided into two parts. We first prove that

$$H = \{ (f:g\sqrt{F}:1) \in E'(K(E)) \mid f,g \in K(X) \} \cup \{O\}$$

is a subgroup of $E'(K(E))$. Since $K(E)$ is a field extension of $K(X)$ of degree 2, there is one non-trivial automorphism σ of $K(E)$ over $K(X)$ defined by $\sqrt{F} \mapsto -\sqrt{F}$. The induced bijection $\sigma: E'(K(E)) \to E'(K(E))$, $\sigma(x:y:z) = (\sigma x:\sigma y:\sigma z)$ is a group automorphism since the addition law is defined by rational functions over K and σ acts trivially on $K(X)$. It is clear that $P \in H$ implies $\sigma P = -P$. Conversely, if $\sigma P = -P$ and $P \neq O$, say $P = (x:y:1)$, then $\sigma x = x$ and $\sigma y = -y$ so $x \in K(X)$, $y \in K(X)\sqrt{F}$ and $P \in H$. Hence

$$H = \{P \in E'(K(E)) \mid \sigma P = -P\},$$

which is a subgroup of $E'(K(E))$ since σ is a homomorphism.
Secondly we prove that

$$\mathrm{Hom}_K(E,E') = \{\ (f{:}g\sqrt{F}{:}1) \in H \mid \deg f_1 > \deg f_2\ \} \cup \{O\}$$

is a subgroup of H. In fact we will show that $\mathrm{Hom}_K(E,E') = \ker h_O \cap H$, which is clearly a subgroup of H. In exercise (2.8) we have seen that the elements in the kernel of the map h defined above are of the form $(x{:}1{:}z)$ with $x,z \in tK[[t]]$. Let $(f{:}g\sqrt{F}{:}1) \in \ker h_O \cap H$. Then

$$\deg i_O(1/g\sqrt{F}) > 0 \Rightarrow$$
$$\deg i_O(g\sqrt{F})^2 = \deg i_O(f^3 + af + b) < 0 \Rightarrow \text{(by exercise (5.2))}$$
$$\deg f_2 - \deg f_1 = \tfrac{1}{2}\cdot\deg i_O(f) < 0\ .$$

So $\ker h_O \cap H \subset \mathrm{Hom}_K(E,E')$. If on the other hand $(f{:}g\sqrt{F}{:}1) \in \mathrm{Hom}_K(E,E')$ then

$$\deg i_O(f) < 0 \Rightarrow$$
$$\deg i_O(g\sqrt{F}) = \tfrac{3}{2}\cdot\deg i_O(f) < 0 \Rightarrow$$
$$\deg i_O(f/g\sqrt{F}) > 0 \text{ and } \deg i_O(1/g\sqrt{F}) > 0\ ,$$

and $\mathrm{Hom}_K(E,E') \subset \ker h_O \cap H$.

(5.5) **Theorem.** Let $\varphi,\psi : E \to E'$ be two morphisms and $P \in E(K)$. Then

$$(\varphi + \psi)(P) = \varphi(P) + \psi(P)\ ,$$

where on the left side the addition is in $E'(K(E))$ and on the right side the addition is in $E'(K)$.

PROOF: Since h_P is a group homorphism we have:

$$(\varphi + \psi)(P) = h_P(\varphi + \psi) = h_P(\varphi) + h_P(\psi) = \varphi(P) + \psi(P)\ .$$

Another proof of (5.5) can be found in exercise (5.3).

(5.6) **Corollary.** Let φ and ψ be morphisms.

(a) If φ and ψ are group homomorphisms then so is $\varphi + \psi$.

(b) Let $E \xrightarrow{\vartheta} E' \xrightarrow{\varphi,\psi} E'' \xrightarrow{\chi} E'''$ be morphisms.
Then $\chi(\varphi + \psi) = \chi\varphi + \chi\psi$ and $(\varphi + \psi)\vartheta = \varphi\vartheta + \psi\vartheta$.

(c) $\mathrm{End}_K(E) = \mathrm{Hom}_K(E,E)$ is a ring with respect to the multiplication given by composition of morphisms, with unit element $1 = [1]$.

PROOF: (a) and (c) are trivial and (b) follows from exercise (5.4).

(5.7) **Definition.** For $m \in \mathbf{Z}$ the multiplication-by-m map $[m]$ is defined as the image of m under the unique unitary ring homomorphism $\mathbf{Z} \to \mathrm{End}_K(E)$.

Let $\underline{m} = tK[[t]]$ be the maximal ideal of $K[[t]]$. By exercise (2.8) there is a group homomorphism $d : \ker h \to \underline{m}/\underline{m}^2 \cong K^+$, the additive group of K, defined by $(x{:}1{:}z) \mapsto (x \bmod t^2)$.

(5.8) **Definition.** Let E,E' be two elliptic curves and $P \in E(K)$. The *derivation map* d_P : $\mathrm{Hom}_K(E,E') \to K$ is the composed map $d_P = d \circ (i_P)_*$. If $\varphi \in \mathrm{Hom}_K(E,E')$ then the *derivative of* φ *at* P is $d_P(\varphi)$.

In an affine neighbourhood of P the tangent line to E at P can be considered as a one dimensional vector space over K with origin at P. Viewed in this way the derivative of φ at P is a K-linear map from the tangent line at P to the tangent line at $\varphi(P)$. Hence the name derivative is not so odd as it may seem. However the derivative is not canonical in the sense that it depends on i_P, which can be defined in many ways to meet our purposes, as well as on the particular isomorphism $\underline{m}/\underline{m}^2 \cong K^+$.

If φ is an isogeny then the embedding $i_P : K(E) \to K((t))$ allows us to extend $\varphi^* : K(E') \to K(E)$ to $K((t))$.

$$\begin{array}{ccc} K((t)) & \dashrightarrow & K((t)) \\ \uparrow{\scriptstyle i_{\varphi(P)}} & & \uparrow{\scriptstyle i_P} \\ K(E') & \xrightarrow{\varphi^*} & K(E) \end{array}$$

The extension $\varphi^*{}_P : K((t)) \to K((t))$ is unique and continuous, i.e. $\varphi^*{}_P(\sum a_i t^i) = \sum a_i \varphi^*{}_P(t)^i$. See exercise (5.7).

(5.9) **Proposition.** Let φ be a morphism.

(a) If φ is an isogeny then $d_O(\varphi) =$ coefficient of $\varphi^*{}_O(t)$ at t.

(b) $d_O(\varphi) = 0$ if $\varphi = O$ or $\varphi = (f : g\sqrt{F} : 1)$ and $\deg f_1 - \deg f_2 > 1$,
and $d_O(\varphi) = \dfrac{\text{leading coefficient of } f_1}{\text{leading coefficient of } g_1}$ otherwise.

PROOF: Exercise (5.8).

(5.10) **Proposition.** Let φ,ψ be morphisms over K.

(a) $d_O(\mathrm{id}_E) = 1$;

(b) $d_O(\varphi + \psi) = d_O(\varphi) + d_O(\psi)$;

(c) $d_O(\varphi \circ \psi) = d_O(\varphi) \cdot d_O(\psi)$;

(d) d_O is a unitary ring homomorphism $\mathrm{End}_K(E) \to K$;

(e) $d_O(\varphi) = 0 \Leftrightarrow \varphi$ is inseparable.

PROOF: (a) Immediate from (5.9.b).

(b) By definition.

(c) This is trivial if $\varphi = O$ or $\psi = O$. If $\varphi, \psi \neq O$ then using (5.9.a) we see that

$$\begin{aligned}(\varphi\circ\psi)^*{}_O(t) &= \psi^*{}_O \circ \varphi^*{}_O(t)\\ &= \psi^*{}_O(\, d_O(\varphi)t + \text{h.o.t.}\,)\\ &= d_O(\varphi)\psi^*{}_O(t) + \text{h.o.t.}\\ &= d_O(\varphi)\cdot d_O(\psi)t + \text{h.o.t.}\,.\end{aligned}$$

(d) Clear from (a), (b) and (c).

(e) Suppose φ is inseparable. If $\operatorname{char} K = 0$ then $\varphi = O$. Since $d_O(\text{Frob}_q) = 0$ by (5.9.b), we obtain the result for $\operatorname{char} K > 0$ from (c) and corollary (4.13).
Conversely, suppose $\varphi = (f:g\sqrt{F}:1)$ is separable and let $m = \deg \varphi$. It will be sufficient to show that $\deg f_2 \geq m - 1$. Denote the algebraic closure of K by L. The point $P = (x:y:1) \in E(L)$ is in the kernel of the induced map $\varphi : E(L) \to E'(L)$ if and only if x is a zero of f_2. This kernel contains exactly m points so the proof is reduced to showing that x is a double root of f_2 if $P \neq -P$. Let $\lambda > 0$ be the multiplicity of x as a root of f_2. The coprimality of f_1 and f_2 implies that the denominator of $f^3 + a'f + b' = g^2F$ has exactly 3λ factors $X - x$. By assumption $X - x$ does not divide F since otherwise $P = -P$. Hence ${g_2}^2$ has 3λ factors $X - x$, so λ is even and therefore $\lambda \geq 2$.

It follows from the proof of (e) that for separable φ the polynomial f_2 can be written as

$$f_2 = \prod_P (X - x_P)\ ,$$

where the product is taken over the non-trivial points $P = (x_P:y_P:1)$ in the kernel of the induced map over the algebraic closure of K. Moreover we see that the inseparable morphisms form a subgroup of $\text{Hom}_K(E,E')$. This subgroup contains $p\cdot\text{Hom}_K(E,E')$ if $\operatorname{char} K = p$, since $d_O(p\varphi) = pd_O(\varphi) = 0$. If $E = E'$ the inseparable morphisms form a two-sided ideal of $\text{End}_K(E)$. In particular we see that if $\operatorname{char} K = 0$ the endomorphism ring of an elliptic curve is isomorphic to a subring of K. Later we shall see that $\text{End}_{\mathbf{Q}}(E) \cong \mathbf{Z}$.

Exercises.

5.1 (a) Let $(f:g:h) \in E'(K(E))$. Show that $h_P(f:g:h) = (f_1g_2h_2(P):f_2g_1h_2(P):f_2g_2h_1(P))$ under suitable conventions.

(b) Show that $h_P(\varphi) = \varphi(P)$.

5.2 (a) The degree function on $K((t))$ is a *discrete valuation*, i.e.

$$\deg(xy) = \deg(x) + \deg(y)\ ;$$

$\deg(x+y) \geq \min\{\deg x, \deg y\}$;

$\deg(x+y) = \min\{\deg x, \deg y\}$ if $\deg x \neq \deg y$.

(b) Show that $K[[t]] = \{ x \in K((t)) \mid \deg x \geq 0 \} \cup \{0\}$ and $tK[[t]] = \{ x \in K((t)) \mid \deg x > 0 \} \cup \{0\}$.

(c) Use (a) and (b) to prove that $tK[[t]]$ is the unique maximal ideal of $K[[t]]$.

(d) Show that $K[[t]]$ is a principal ideal domain.

5.3 Let $\varphi, \psi \in \mathrm{Hom}_K(E,E')$ and $\alpha, \beta : E(K) \to E'(K)$ be the homomorphisms $P \mapsto (\varphi+\psi)(P)$ and $P \mapsto \varphi(P) + \psi(P)$.

(a) Use lemma (1.5) to show that $\alpha(P) = \beta(P)$ for almost every (i.e. for all but finitely many) $P \in E(L)$.

(b) If $L \supset K$ is a field such that $E(L)$ is infinite then $\{ P \in E(L) \mid \alpha(P) = \beta(P) \} = E(L)$.

(c) Prove theorem (5.6).

Remark: note that this proof uses theorem (4.6) whereas the proof in the text does not.

5.4 Let $\varphi, \psi : E \to E'$ be two morphisms over K . Show that the following are equivalent:

(a) $\varphi = \psi$;

(b) The induced maps $\varphi : E(L) \to E'(L)$ and $\psi : E(L) \to E'(L)$ are equal for every field extension $L \supset K$;

(c) The induced maps $\varphi : E(\overline{K}) \to E'(\overline{K})$ and $\psi : E(\overline{K}) \to E'(\overline{K})$ are equal.

5.5 Let $c \in \mathbf{R}_{>1}$ and $d : K((t)) \times K((t)) \to \mathbf{R}_{\geq 0}$ be defined as

$$d(x,y) = \begin{cases} c^{-\deg(x-y)} & \text{if } x \neq y ; \\ 0 & \text{if } x = y . \end{cases}$$

(a) Show that d is a metric function on $K((t))$.

(b) Show that $(K((t)),d)$ is a complete metric space.

(c) Hence if $x \in tK[[t]]$ and $a_i \in K$ for $i \geq i_0$ the sum

$$\sum_{i \geq i_0} a_i x^i \;:=\; \lim_{n \to \infty} \sum_{i=i_0}^{n} a_i x^i$$

is well defined and

$$\sum_{i \geq i_0} a_i x^i \;=\; \sum_{i=i_0}^{n} a_i x^i \;+\; \sum_{i>n} a_i x^i \quad \text{for all } n \geq i_0 .$$

(d) Show that if $\deg x = 1$ every element of $K((t))$ can be written as a sum $\sum a_i x^i$.

5.6 (a) Show that $K[[t]]^* = K^* \cdot \{ y \in K((t))^* \mid \forall n \geq 0 \; \exists z \in K((t)) : z^{2^n} = y \}$.

(b) Let $f : K((t)) \to K((t))$ be a homomorphism of fields such that $f_{|K} = \mathrm{id}_K$. Show that $f(K[[t]]) \subset K[[t]]$ and $f(t) \in tK[[t]]$. (Hint: $K[[t]] = K[[t]]^* + K[[t]]^*$.)

(c) $f(\sum a_i t^i) - \sum a_i f(t)^i \in t^n K[[t]]$ for all $n \geq 0$.

(d) Conclude that f is uniquely determined by $f(t)$.

(e) Show that f is a continuous function $(K((t)),d) \to (K((t)),d)$.

5.7 (a) Let x,y be elements of $K((t))^*$ with degrees $a,b \neq 0$ respectively, such that $\gcd(a,b) = 1$. Then there exist elements $\lambda,\mu \in \mathbf{Z}$ such that $\deg x^\lambda y^\mu = 1$.

(b) Let $\varphi : E \to E'$ be an isogeny. Show that φ^*_P is uniquely defined. [Hint: use exercises (5.5) and (5.6).]

5.8 (a) Prove proposition (5.9).

(b) Show that $d_O(u) = u$ if u is an isomorphism (considered as an element of K^* as in section 1).

5.9 Let E be an elliptic curve over K and $[m]$ the multiplication-by-m map for $m \in \mathbf{Z}$. Show that:

(a) $[m]$ is a morphism ;

(b) $\mathrm{End}_K(E)$ does not have zero-divisors ;

(c) $[2]$ is not a unit in $\mathrm{End}_K(E)$;

(c) $[m]$ is an isogeny if $m \neq 0$ [Hint: consider the ring homomorphism $\mathbf{Z} \to \mathrm{End}_K E$] .

5.10 Prove that $\deg \varphi^*{}_O(t) = [\, K((t)) : \varphi^*{}_O K((t)) \,] = \deg_i \varphi$. Hence $\varphi^*{}_O$ is bijective if and only if φ is separable.

§6. Elliptic curves over the field of complex numbers.

In this somewhat informal section we intend to give an illustration of how analytic methods can give deep insight into the theory of elliptic curves. No proofs are given for the main results, not because they are difficult (in fact they require no more then a first year's course in calculus of one complex variable), but rather because the ingredients do not fit into our algebraic approach. Detailed proofs, and many more interesting facts about this vast subject can be found in Koblitz [10]. The corollaries in this section will be proved later for general fields, by means of algebraic techniques. For these reasons this section may seem superfluous, but one might have felt deceived if this classical approach would not have been treated. Moreover it is very instructive to see the correspondence lattice $\leftrightarrow$ elliptic curve.

(6.1) **Definition.** A *lattice* in $\mathbf{C}$ is a subgroup L of the additive group $\mathbf{C}^+$ of the form

$$L = \mathbf{Z}\alpha + \mathbf{Z}\beta ,$$

where $\alpha,\beta \in \mathbf{C}^*$ are linearly independent over $\mathbf{R}$. Two lattices L and L' are *homothetic* if $L = \alpha L'$ for some $\alpha \in \mathbf{C}^*$, and *isogenous* if $L \subset \alpha L'$ for some $\alpha \in \mathbf{C}^*$. (This is indeed an equivalence relation: see exercise(6.1).)

(6.2) **Definition.** Let L be a lattice in $\mathbf{C}$. The *Weierstrass $\wp$-function* associated to L is

$$\wp(z;L) = z^{-2} + \sum_{\omega \in L-\{0\}} \{ (z-\omega)^{-2} - \omega^{-2} \} .$$

The derivative of $\wp$ is

$$\wp'(z;L) = -2 \sum_{\omega \in L} (z-\omega)^{-3} .$$

We will write $\wp(z)$ for short when the reference to L is clear. The correction term ω^{-2} in the representation of $\wp(z)$ is needed to make the series convergent.

(6.3) **Proposition.** The Weierstrass $\wp$-function $\wp(z;L)$ satisfies the following properties:

(a) it is meromorphic ;
(b) it has a pole of order 2 in all the points of L and no others ;
(c) it is periodic with respect to L, i.e. $\wp(z+\omega;L) = \wp(z;L)$ for all $\omega \in L$;
(d) it is even, i.e. $\wp(-z;L) = \wp(z;L)$.

Its derivative $\wp'(z;L)$ satisfies:

(a) it is meromorphic ;
(b) it has a pole of order 3 in all the points of L and no others ;
(c) it is periodic with respect to L ;
(d) it is odd, i.e. $\wp'(-z;L) = -\wp'(z;L)$.

Furthermore the Weierstrass $\wp$-function satisfies a functional equation:

$$\wp'(z)^2 = 4\wp(z)^3 - 60g_4\wp(z) - 140g_6 \text{ , where}$$

$$g_i = g_i(L) = \sum_{\omega \in L-\{0\}} \omega^{-i} \text{ for } i = 4,6.$$

PROOF: Koblitz [10, sections I.4-6].

(6.4) **Definition.** Let L be a lattice in $\mathbf{C}$. The elliptic curve associated to L is

$$E_L = E_{-15g_4(L),-35g_6(L)} .$$

There is a canonical map $\mathbf{C} \to E_L(\mathbf{C})$ defined by

$$z \mapsto \begin{cases} (\wp(z) : {}^1\!/_2\wp'(z) : 1) & \text{if } z \notin L ; \\ (0 : 1 : 0) & \text{if } z \in L . \end{cases}$$

(6.5) **Theorem.**

(a) Let L be a lattice in $\mathbf{C}$. The map $\mathbf{C}/L \to E_L(\mathbf{C})$ induced by the map above is an isomorphism of abelian groups. The group of points $E_L(\mathbf{C})$ is isomorphic to $(\mathbf{R} \times \mathbf{R}) / (\mathbf{Z} \times \mathbf{Z}) \cong \mathbf{T} \times \mathbf{T}$, where $\mathbf{T}$ denotes the circle group $\mathbf{T} = \{ e^{ix} \mid x \in \mathbf{R} \}$.

(b) There is a one-to-one correspondence between elliptic curves over $\mathbf{C}$ and lattices in $\mathbf{C}$, given by $E_L \leftrightarrow L$.

(c) Let L,L' be lattices and $\alpha \in \mathbf{C}$ such that $\alpha L \subset L'$. Then there is a unique morphism $\varphi_\alpha : E_L \to E_{L'}$ such that the following diagram is commutative:

$$\begin{array}{ccc} \mathbf{C}/L & \longrightarrow & E_L(\mathbf{C}) \\ \downarrow \alpha & & \downarrow \varphi_\alpha \\ \mathbf{C}/L' & \longrightarrow & E_{L'}(\mathbf{C}) \end{array}$$

Here the map $\mathbf{C}/L \to \mathbf{C}/L'$ is given by $z \bmod L \mapsto \alpha z \bmod L'$.

(d) The map $\alpha \mapsto \varphi_\alpha$ is a group isomorphism $\{ \alpha \in \mathbf{C} \mid \alpha L \subset L' \} \cong \mathrm{Hom}_{\mathbf{C}}(E_L, E_{L'})$. Also $\varphi_{\alpha\beta} = \varphi_\alpha \circ \varphi_\beta$ whenever this expression makes sense. The inverse of this map is the derivation map: $d_O(\varphi_\alpha) = \alpha$.

PROOF: (a) Silverman [19, section VI.3] ;

(b) Koblitz [10, section III.2] ;

(c) Silverman [19, section VI.4] ;

(d) Silverman [19, section VI.5] .

In fact the isomorphism in (a) is an analytic isomorphism. In particular an elliptic curve over $\mathbf{C}$ is a torus embedded in the four-dimensional real space. This explains the terminology "genus 1" as

indicated in section 1: an elliptic curve has one hole.

(6.6) **Corollary.**

(a) The group of m-torsion points $E(\mathbf{C})[m] = \{ P \in E(\mathbf{C}) \mid mP = O \}$ of an elliptic curve is isomorphic to $\mathbf{Z}/m\mathbf{Z} \times \mathbf{Z}/m\mathbf{Z}$.

(b) If $\varphi = \varphi_\alpha$ is an isogeny $E_L \to E_{L'}$ then $\deg \varphi = \#\ker \varphi_\alpha = \#\ker \alpha = \text{index}[L' : \alpha L]$.

(c) Two elliptic curves are isomorphic if and only if the corresponding lattices are homothetic.

PROOF: (a) Immediate from (6.5). In the next section we will deduce a similar result (for general algebraically closed fields) by algebraic arguments.

(b) Clear.

(c) Two curves E and E' are isomorphic if and only if there exist morphisms $\varphi : E \to E'$ and $\psi : E' \to E$ such that $\varphi \circ \psi = \text{id}_{E'}$ and $\psi \circ \varphi = \text{id}_E$. Now apply (6.5.d).

We will now study the endomorphism ring of an elliptic curve more closely. By a *discrete* subring of $\mathbf{C}$ we mean a subring that inherits the discrete topology as a subset of $\mathbf{C}$.

(6.7) **Theorem.** Let R be a discrete subring of $\mathbf{C}$.

(a) Either $R = \mathbf{Z}$ or $R = \mathbf{Z} + \mathbf{Z}\alpha$, where $\alpha \in \mathbf{C}$ satisfies $\alpha^2 + m\alpha + n = 0$ with $m = 0$ or 1 and $n \in \mathbf{Z}_{\geq 1}$.

(b) If $\beta \in R$ then $\overline{\beta} \in R$, i.e. R is closed under complex conjugation.

PROOF: The polynomial in (a) has discriminant < 0, so if α is a root of it then $\alpha \notin \mathbf{R}$ and $\alpha^2 \in \mathbf{Z} + \mathbf{Z}\alpha$, so $\mathbf{Z} + \mathbf{Z}\alpha$ is a discrete subring of $\mathbf{C}$, as well as $\mathbf{Z}$. Conversely any subring of $\mathbf{C}$ contains $\mathbf{Z}$ and in a discrete subring every real element is an integer, for otherwise the ring would contain an element $0 < x < 1$ which has the property $x^n \to 0$ if n grows, a contradiction. Now suppose $R \neq \mathbf{Z}$. Then there exists $\alpha \in R$ with

$$\text{Im } \alpha > 0 \text{ minimal} \quad \text{and} \quad {}^1\!/_2 \leq \text{Re } \alpha < {}^1\!/_2 .$$

Let $x \in R$ be arbitrary and take $k \in \mathbf{Z}$ such that

$$0 \leq \text{Im } (x - k\alpha) < \text{Im } \alpha .$$

The minimality of $\text{Im } \alpha$ implies that $\text{Im}(x - k\alpha) = 0$. So $x - k\alpha \in \mathbf{Z}$ and hence $x \in \mathbf{Z} + \mathbf{Z}\alpha$. This proves $R \subset \mathbf{Z} + \mathbf{Z}\alpha$. The other inclusion is obvious. It follows that

$$\alpha\overline{\alpha} - (\alpha + \overline{\alpha})\alpha = -\alpha^2 = n + m\alpha \qquad \text{for some } n,m \in \mathbf{Z},$$

and we see that $m = -(\alpha + \overline{\alpha}) = -2\text{Re}(\alpha)$, so $-1 < m \leq 1$ and $n = \alpha\overline{\alpha} = |\alpha|^2 > 0$.

If $\beta \in R$ then by the same reason as above $\beta + \overline{\beta}$ and $\beta\overline{\beta} \in R$, in particular $\overline{\beta} \in R$.

(6.9) **Theorem.**

(a) Let E be the elliptic curve over $\mathbf{C}$ corresponding to the lattice $L = \mathbf{Z}x + \mathbf{Z}y$. Then $\mathrm{End}_{\mathbf{C}}(E)$ is isomorphic to a discrete subring of $\mathbf{C}$. If we write $\mathbf{Q}(L) =_{\mathrm{def}} \mathbf{Q}(x/y)$ then this subring is *not* equal to $\mathbf{Z}$ if and only if $\mathbf{Q}(L)$ is a quadratic extension of $\mathbf{Q}$. In fact $\mathrm{End}_{\mathbf{C}}(E)$ is isomorphic to a discrete subring of $\mathbf{Q}(L)$.

(b) Let E,E' be elliptic curves over $\mathbf{C}$ corresponding to lattices L and L'.

$$\mathrm{Hom}_{\mathbf{C}}(E,E') \cong \begin{cases} \mathbf{Z}\times\mathbf{Z} & \text{if } L \text{ and } L' \text{ are isogenous and } [\mathbf{Q}(L):\mathbf{Q}] = 2\,; \\ \mathbf{Z} & \text{if } L \text{ and } L' \text{ are isogenous and } [\mathbf{Q}(L):\mathbf{Q}] > 2\,; \\ 0 & \text{otherwise}. \end{cases}$$

PROOF: (a) Exercise (6.2).

(b) This follows from (a) once we have noted that the isomorphism class of $\mathrm{Hom}_{\mathbf{C}}(E,E')$ as an abelian group only depends on the isogeny classes of E and E', since in that case $\mathrm{Hom}_{\mathbf{C}}(E,E') \cong \mathrm{End}_{\mathbf{C}}(E)^+$ if E and E' are isogenous, and 0 otherwise. Let M,M' be lattices isogenous to L,L' respectively, say $\beta M \subset L$ and $\beta' L' \subset M'$. If $\alpha L \subset L'$ then

$$\beta'\alpha\beta M \subset \beta'\alpha L \subset \beta' L' \subset M'.$$

So the map $\alpha \mapsto \beta'\alpha\beta$ is an injection $\{\alpha \in \mathbf{C} \mid \alpha L \subset L'\} \to \{\alpha \in \mathbf{C} \mid \alpha M \subset M'\}$. If we take $M = M' = L$ we see that $\mathrm{Hom}_{\mathbf{C}}(E,E')$ is isomorphic to a subgroup of $\mathrm{End}_{\mathbf{C}}(E)^+ \cong (\mathbf{Z}\times\mathbf{Z}$ or $\mathbf{Z})$ and as such is either $0, \mathbf{Z}$ or $\mathbf{Z}\times\mathbf{Z}$. By reasons of symmetry $\mathrm{End}_{\mathbf{C}}(E)^+$ is isomorphic to a subgroup of $\mathrm{Hom}_{\mathbf{C}}(E,E')$ which is only possible if the two are isomorphic.

(6.10) **Definition.** Let $R \neq \mathbf{Z}$ be a discrete subring of $\mathbf{C}$.

(a) The *discriminant* of R, denoted Δ_R, is defined as $\Delta_R = (\alpha - \overline{\alpha})^2$, where α is as in (6.7).

(b) The *class number* of R, denoted h_R, is defined as

$$h_R = \#\{(a,b,c) \in \mathbf{Z}^3 \mid \gcd(a,b,c) = 1,\ b^2 - 4ac = \Delta_R,\ |b| \le a \le c, \text{ and } b \ge 0 \text{ if } |b| = a \text{ or } a = c\}.$$

(6.11) **Theorem.** Let $R \neq \mathbf{Z}$ be a discrete subring of $\mathbf{C}$. Then

$$\#\{E/\mathbf{C} \mid \mathrm{End}_{\mathbf{C}} E \cong R\}/\cong_{\mathbf{C}} \;=\; h_R.$$

PROOF: By theorem (6.5) we have to show that

$$h_R = \#\{L \text{ lattice} \mid R = \{z \in \mathbf{C} \mid zL \subset L\}\}/\mathbf{C}^*.$$

By exercise (6.4) every lattice is homothetic to a unique lattice of the form $L = \mathbf{Z} + \mathbf{Z}\gamma$ where $\gamma \in \mathbf{C}$ satisfies

$$\mathrm{Im}\,\gamma > 0\ ,\ |\gamma| \ge 1\ ,\ -\tfrac{1}{2} < \mathrm{Re}\,\gamma \le \tfrac{1}{2} \text{ and } \mathrm{Re}\,\gamma \ge 0 \text{ if } |\gamma| = 1.$$

Furthermore exercise (6.4) states that there exist $a,b,c \in \mathbf{Z}$ such that

$$a\gamma^2 - b\gamma + c = 0 \text{ and } \gcd(a,b,c) = 1,$$

and we may take $a > 0$ by changing signs, if necessary. Finally exercise (6.4) shows that

$$\mathbf{Z}[\alpha] = \mathbf{Z}[a\gamma] .$$

where α is as in theorem (6.7). Comparing imaginary parts we see that $a\sqrt{b^2-4ac}/2a = \text{Im } \alpha$ and hence $b^2 - 4ac = 4(\text{Im } \alpha)^2 = \Delta_R$. The conditions on γ imply that $|b| \le a \le c$ and $b \ge 0$ if one of the inequalities is an equality. Finally any triple (a,b,c) such as in (6.10) induces a zero γ of the polynomial $aX^2 - bX + c$ that is of the required form.

The following theorem will be used in the analysis of the algorithms in sections 11 and 12.

(6.12) **Theorem.** (Brauer-Siegel)

$$h_R = |\Delta_R|^{1/2+o(1)} \text{ for } \Delta_R \to -\infty .$$

PROOF: Lang [12, chapter XVI] ; see also exercise (6.5).

Exercises.

6.1 Let L,L' be lattices and $\alpha \in \mathbf{C}^*$ such that $\alpha L \subset L'$. Show that there exists $\alpha' \in \mathbf{C}^*$ such that $\alpha' L' \subset L$. Show that α' can be chosen such that $\alpha\alpha' = \deg \varphi_\alpha$.

6.2 Let $E = E_L$ be the elliptic curve associated to $L = \mathbf{Z}x + \mathbf{Z}y$.

(a) Show that $\text{End}_{\mathbf{C}}(E)$ is isomorphic to a discrete subring of $\mathbf{C}$.

(b) Suppose $\text{End}_{\mathbf{C}}(E) \cong \mathbf{Z} + \mathbf{Z}\alpha$. Show that there exist integers $a,b,c,d \in \mathbf{Z}$ such that $\alpha = a + bx/y$ and $\alpha x/y = c + dx/y$.

(c) Prove theorem (6.9.a).

6.3 (a) Let $E = E_{a,0}$ with $a \in \mathbf{C}^*$. Show that $\text{End}_{\mathbf{C}}(E) \cong \mathbf{Z}[i]$.

(b) Let $E = E_{0,b}$ with $b \in \mathbf{C}^*$. Show that $\text{End}_{\mathbf{C}}(E) \cong \mathbf{Z}[\zeta_3]$, where ζ_3 is a primitive third root of unity.

6.4 (a) Show that every lattice is homothetic to a unique lattice of the form $\mathbf{Z} + \mathbf{Z}\gamma$, where γ is as in the proof of theorem (6.11).

Let $L = \mathbf{Z} + \mathbf{Z}\gamma$ and $R = \{ z \in \mathbf{C} \mid zL \subset L \}$. Suppose that $R \neq \mathbf{Z}$.

(b) Show that there exist $a,b,c \in \mathbf{Z}$ with $\gcd(a,b,c) = 1$, such that $a\gamma^2 - b\gamma + c = 0$.

Let $L' = \mathbf{Z} + \mathbf{Z}\overline{\gamma}$ and $R' = \mathbf{Z}[a\gamma]$.

(c) Show that $aL \cdot L' = R'$.

(d) Show that $R' = R$.

6.5 Show that $h_R \le |\Delta_R|^{1/2+o(1)}$.

§7. The degree as a quadratic form.

In this section we will derive some properties of the map $\deg : \mathrm{Hom}_K(E,E') \to \mathbf{Z}$ and as a result we shall be able to give an upper and lower bound of the number of points on an elliptic curve over a finite field.

(7.1) **Proposition.** Let E,E' be two elliptic curves over K and $\varphi,\psi \in \mathrm{Hom}_K(E,E')$. Then

$$\deg(\varphi+\psi) + \deg(\varphi-\psi) = 2\deg\varphi + 2\deg\psi .$$

PROOF: It will be enough to show $\deg(\varphi+\psi) + \deg(\varphi-\psi) \le 2\deg\varphi + 2\deg\psi$, since by substitution of $\varphi+\psi$ for φ and $\varphi-\psi$ for ψ it then follows that

$$4(\deg\varphi + \deg\psi) = \deg(2\varphi) + \deg(2\psi) \le 2\deg(\varphi+\psi) + 2\deg(\varphi-\psi),$$

and we obtain the inequality in the opposite direction. Here we use that $\deg 2 = 4$, see exercise (4.4). The cases $\varphi,\psi,\varphi+\psi$ or $\varphi-\psi = O$ being trivial, we may assume $\varphi = (f:g\sqrt{F}:1)$, $\psi = (h:j\sqrt{F}:1)$ with $f \neq h$ and put $\varphi+\psi = (k_+:\ldots:1)$, $\varphi-\psi = (k_-:\ldots:1)$. Using (1.3) and the equalities $g^2F = f^3+a'f+b'$ and $j^2F = h^3+a'h+b'$ we find

$$k_{-/+} = \left(\frac{g\pm j}{f-h}\right)^2 - f - h$$

$$= \frac{(g\pm j)^2F - (f+h)(f-h)^2}{(f-h)^2}$$

$$= \frac{\pm 2gjF + (f+h)(fh+a') + 2b'}{(f-h)^2} .$$

The denominator of $g^2F\cdot j^2F$ divides $(f_2h_2)^3$ and therefore the denominator of gjF divides $(f_2h_2)^2$. It follows that $k_\pm = T_\pm / N$, with

$$T_{-/+} = (f_2h_2)^2\cdot(\pm 2gjF + (f+h)(fh+a') + 2b') \in K[X],$$

and

$$N = (f_1h_2 - f_2h_1)^2 \in K[X] .$$

On the other hand a little calculation shows that

$$k_+\cdot k_- = \frac{(f+h)^2(fh+a')^2 + 4b'(f+h)(fh+a') + 4b'^2 - 4(gjF)^2}{(f-h)^4}$$

$$= \Big[\ (f^4h^2 - f^3h^3 + f^2h^4) - 2a'(f^3h - 2f^2h^2 + fh^3)$$
$$- 4b'(f^3 - f^2h - fh^2 + h^3) + a'^2(f^2 - 2fh + h^2)\ \Big](f-h)^{-4}$$

$$= \frac{(f^2h^2 - 2a'fh - 4b'(f+h) + a'^2)(f-h)^2}{(f-h)^4}$$

$$= \frac{(fh - a')^2 - 4b'(f+h)}{(f-h)^2}$$

$$= \frac{(f_1h_1 - a'f_2h_2)^2 - 4b'(f_1h_2 + f_2h_1)f_2h_2}{N} = \frac{\text{polynomial}}{N} \quad .$$

From $k_+k_- = T_+T_-/N^2$ it follows that N divides $T_+T_- \in K[X]$. We now have

$$N = \gcd(T_+T_- , N) \mid \gcd(T_+ , N)\cdot\gcd(T_- , N)$$

so

$$\begin{aligned}
\deg(\varphi + \psi) + \deg(\varphi - \psi) &= \deg T_+ - \deg(\gcd(T_+ , N)) + \deg T_- - \deg(\gcd(T_- , N)) \\
&\le \deg(T_+T_-) - \deg(\gcd(T_+T_- , N)) \\
&= \deg(T_+T_-) - \deg N \\
&= \deg[\ (f_1h_1 - a'f_2h_2)^2 - 4b'(f_1h_2 + f_2h_1)f_2h_2\ ] \\
&= \deg(f_1h_1)^2 \\
&= 2\deg\varphi + 2\deg\psi \ ,
\end{aligned}$$

which concludes the proof.

(7.2) **Corollary.** The degree of the multiplication-by-m map is $\deg[m] = m^2$.

PROOF: By the proposition $\deg[m+1] + \deg[m-1] = 2\deg[m] + 2\deg[1]$, so by induction $\deg[m+1] = 2m^2 - (m-1)^2 + 2 = (m+1)^2$.

Notation: If A is an (additive) abelian group and $m \in \mathbf{Z}_{>0}$ we denote by $A[m]$ the subgroup of m-torsion elements of A, i.e. $A[m] = \{\ x \in A \mid mx = 0\ \}$.

(7.3) **Corollary.** Let E be an elliptic curve over K and $m \in \mathbf{Z}_{>0}$.

(a) If $\mathrm{char}(K) \dagger m$ then

$$E(\overline{K})[m] \cong (\mathbf{Z}/m\mathbf{Z}) \times (\mathbf{Z}/m\mathbf{Z}) .$$

(b) If $\mathrm{char}(K) = p > 0$ and $m = p^kn$, with $k > 0$ and $p \dagger n$ then for some $i \in \{0,1\}$, which depends only on E and not on m, we have

$$E(\overline{K})[m] \cong (\mathbf{Z}/\ p^k\mathbf{Z})^i \times (\mathbf{Z}/n\mathbf{Z}) \times (\mathbf{Z}/n\mathbf{Z}) .$$

PROOF: (a) Let d be a divisor of m. It is clear that $E(\overline{K})[m][d] = E(\overline{K})[d] = \ker[d]$ so $\#E(\overline{K})[d] = \deg_s[d]$. Since $\mathrm{char}(K) \dagger d$ it follows from proposition (5.10.e) that $[d]$ is separable and so $\#E(\overline{K})[d] = \deg[d] = d^2$. Now apply exercise (7.1.b).

(b) Using (5.10.e) again we see that $[p]$ is inseparable. Hence $\deg_s[p]$ is a strictly smaller

divisor of $\deg[p] = p^2$, say $\deg_s[p] = p^i$. Since $E(\overline{K})[p]$ is the kernel of the map $[p] : E(\overline{K})[p^k] \to E(\overline{K})[p^{k-1}]$ and in general isogenies over algebraically closed fields are surjective, it follows by induction that $\#E(\overline{K})[p^k] = p^{ik}$. The general result follows from (a) and exercise (7.1.a and b).

(7.4) **Definition.** An elliptic curve E/K is called *super-singular* if $\operatorname{char} K = p > 0$ and the following equivalent properties hold:

(a) $E(\overline{K})[p^k] = \{O\}$;

(b) $[p]$ is purely inseparable ;

(c) $[p]_{\text{sep}}$ is an isomorphism and $[p] = [p]_{\text{sep}} \circ \text{Frob}_{p^2}$.

Super-singular curves are rare: because $[p]_{\text{sep}}$ is an isomorphism a necessary condition for $E_{a,b}$ to be super-singular is $E_{a,b} \cong E_{a^{p^2},b^{p^2}}$.
This implies $j(E) = j(E)^{p^2}$, so $j(E) \in \mathbf{F}_{p^2}$. The converse is not true (for example a curve E defined over $\mathbf{F}_p$ has $j(E) \in \mathbf{F}_p$ but clearly need not be super-singular). In fact it can be shown that if K is an algebraically closed field of characteristic $p > 3$ the number of supersingular curves over K is

$$[p/12] + \begin{cases} 0 \text{ if } p \equiv 1 \pmod{12} \\ 1 \text{ if } p \equiv 5 \text{ or } 7 \pmod{12} \\ 2 \text{ if } p \equiv 11 \pmod{12} \end{cases}$$

(7.5) **Proposition.** The map $(\ ,\ ) : \text{Hom}_K(E,E') \times \text{Hom}_K(E,E') \to \mathbf{Z}$ defined by

$$(\varphi,\psi) = \deg(\varphi+\psi) - \deg(\varphi) - \deg(\psi)$$

is bilinear, symmetric and $\|\varphi\| := (\varphi,\varphi) = 2\deg\varphi$.

PROOF: Symmetry is trivial and $\|\varphi\| = \deg(2\varphi) - 2\deg(\varphi) = 2\deg(\varphi)$. As for bilinearity, we have the following series of identities using (7.1) several times:

$$\begin{aligned} 4\deg(\varphi+\psi+\chi) &= \deg((\varphi+2\psi) + (\varphi+2\chi)) \\ &= 2\deg(\varphi+2\psi) + 2\deg(\varphi+2\chi) - 4\deg(\psi-\chi) \\ &= 2\deg((\varphi+\psi) + \psi) + 2\deg((\varphi+\chi) + \chi) - 4\deg(\psi-\chi) \\ &= \quad 4\deg(\varphi+\psi) + 4\deg(\psi) - 2\deg(\varphi) \\ &\quad + 4\deg(\varphi+\chi) + 4\deg(\chi) - 2\deg(\varphi) \\ &\quad + 4\deg(\psi+\chi) - 8\deg(\psi) - 8\deg(\chi) . \end{aligned}$$

Rearranging terms and dividing by 4 yields

$$\begin{aligned} (\varphi,\psi+\chi) &= \deg(\varphi+\psi+\chi) - \deg(\varphi) - \deg(\psi+\chi) \\ &= \deg(\varphi+\psi) - 2\deg(\varphi) - \deg(\psi) - \deg(\chi) + \deg(\varphi+\chi) \\ &= (\varphi,\psi) + (\varphi,\chi) , \end{aligned}$$

whence the pairing is bilinear.

(7.6) **Theorem.** (Hasse, 1934). Let E be an elliptic curve over $K = \mathbf{F}_q$. Then
$$|\, \#E(\mathbf{F}_q) - (q+1)\,| \leq 2\sqrt{q}\,.$$

Remark: note that $q + 1 = \#\mathbf{P}^1(\mathbf{F}_q)$.

PROOF: Let $\varphi = \mathrm{Frob}_q : E \to E^{(q)} = E$ be the Frobenius morphism. The points over K are characterized by $E(K) = \{\, P \in E(\overline{K}) \mid \varphi P = P \,\} = \ker\{\varphi - 1 : E(\overline{K}) \to E(\overline{K})\,\}$. Indeed, if $\varphi(x{:}y{:}1) = (x^q{:}y^q{:}1) = (x{:}y{:}1)$ then $x = x^q$ and $y = y^q$, so $(x,y) \in \mathbf{F}_q \times \mathbf{F}_q$. Since $d_O(\varphi-1) = d_O(\varphi)+d_O(1) = 1$ we see by proposition (5.10.e) that $\varphi-1$ is separable, and so
$$\#E(K) = \deg_s(\varphi-1) = \deg(\varphi-1) = {}^1\!/_2\, \|\varphi\|\,.$$
For arbitrary $m,n \in \mathbf{Z}$ we have
$$\begin{aligned} \deg(m\varphi + n) &= {}^1\!/_2\, \|m\varphi + n\| \\ &= {}^1\!/_2 m^2(\varphi,\varphi) + mn(\varphi,1) + {}^1\!/_2 n^2(1,1) \\ &= m^2 q + mn(\varphi,1) + n^2\,. \end{aligned}$$
Applying this to $m = 2$, $n = -(\varphi,1)$ we get $0 \leq \deg(m\varphi + n) = 4q - (\varphi,1)^2$, so $|(\varphi,1)| \leq 2\sqrt{q}$. Taking $m = 1$, $n = 1$ yields $\deg(\varphi-1) = q - (\varphi,1) + 1$, so $|\#E(\mathbf{F}_q) - (q+1)| = |(\varphi,1)|$.

Exercises.

7.1 Let A be an abelian group.

(a) If $m,n \in \mathbf{Z}_{>0}$ are coprime then $A[mn] \cong A[m] \times A[n]$.

(b) Let $\#A = m^k$, where $m \in \mathbf{Z}_{>0}$, $k \in \mathbf{Z}_{\geq 0}$ and suppose $\#A[d] = d^k$ for all $d \mid m$. Then $A \cong (\mathbf{Z}/m\mathbf{Z})^k$.

7.2 Let E,E' be elliptic curves and denote the first coordinate of a non-zero element $\varphi \in \mathrm{Hom}_K(E,E')$ by x_φ, with numerator and denominator $(x_\varphi)_1$ and $(x_\varphi)_2$ respectively. Now suppose $\varphi,\psi \neq O$ and $\varphi \neq \pm\psi$. Prove that
$$(x_{\varphi+\psi})_2 \cdot (x_{\varphi-\psi})_2 = \lambda((x_\varphi)_1 \cdot (x_\psi)_2 - (x_\varphi)_2 \cdot (x_\psi)_1) \quad \text{for some } \lambda \in K^*\,.$$

§8. The division polynomial.

This section is devoted entirely to the construction of the division polynomials, which give explicit formulae for the morphisms $[m]$. We fix an elliptic curve $E = E_{a,b}$ over a field K and denote by F the polynomial $F = X^3 + aX + b$.

(8.1) **Definition.** The *division polynomials* $\psi_m \in K[X,\sqrt{F}] = K[X] \oplus K[X]\sqrt{F}$, for $m \in \mathbf{Z}_{\geq -1}$, are defined inductively as follows:

$$\psi_{-1} = -1 ;$$
$$\psi_0 = 0 ;$$
$$\psi_1 = 1 ;$$
$$\psi_2 = 2\sqrt{F} ;$$
$$\psi_3 = 12F\cdot X - (F')^2 = 3X^4 + 6aX^2 + 12bX - a^2 ;$$
$$\psi_4 = 4\sqrt{F}(F'\cdot\psi_3 - 8F^2) = 4\sqrt{F}(X^6 + 5aX^4 + 12bX^3 - 5a^2X^2 + 4abX - 8b^2 - a^3) ;$$
$$\dots$$
$$\psi_{2m+1} = \psi_{m+2}(\psi_m)^3 - \psi_{m-1}(\psi_{m+1})^3 \quad (m \geq 2) ;$$
$$\psi_{2m} = \psi_m(\psi_{m+2}(\psi_{m-1})^2 - \psi_{m-2}(\psi_{m+1})^2) / (2\sqrt{F}) \quad (m \geq 3) .$$

(8.2) **Theorem.** Let $m \in \mathbf{Z}_{\geq 1}$. Then

(a) $$[m] = \left(X - \frac{\psi_{m-1}\psi_{m+1}}{\psi_m^{\,2}} \;:\; \frac{(\psi_{m+2}(\psi_{m-1})^2 - \psi_{m-2}(\psi_{m+1})^2) / (4\sqrt{F})}{\psi_m^{\,3}} \;:\; 1 \right) \qquad (*)$$

(Here the numerators and denominators of the two fractions are coprime polynomials.)

(b) $(\psi_m)^2 = \lambda\cdot\prod(X - x_P)^{\deg_i[m]}$, where $\lambda \in K^*$ and the product is taken over all $P = (x_P:y_P:1) \in E(\overline{K})$ such that $mP = O \neq P$.

PROOF: Since $[m]$ is invariant under field extensions we may assume $K = \overline{K}$. We first deal with the case char $K = 0$. Define another set of polynomials φ_m, $m \in \mathbf{Z}_{\geq -1}$ by $\varphi_0 = 0$ and for $m \neq 0$

$$\varphi_m = m \cdot \left\{ \begin{matrix} \sqrt{F} \text{ if } m \text{ even} \\ 1 \text{ if } m \text{ odd} \end{matrix} \right\} \cdot \prod\{ (X - x) \mid \exists y \in K^* : m(x:y:1) = O \} .$$

It is clear that $\varphi_m^{\,2} = m^2 \cdot \prod_{P \in \ker[m] - \{O\}} (X - x_P) \quad \in \quad K[X]$.

If $[m] = (f_m : g_m\sqrt{F} : 1)$ then the denominator of f_m is $\varphi_m^{\,2}$. Denote

$$h_m = \varphi_m^{\,2}\cdot(X - f_m) = \varphi_m^{\,2}\cdot X - (\text{numerator of } f_m) \in K[X] .$$

We shall prove that $h_m = \varphi_{m+1}\varphi_{m-1}$. Since $d_O[m] = m \neq 0$ and $\deg \varphi_m^{\,2} = m^2 - 1$ it follows by proposition (5.9) that

$$\deg h_m = \deg(\text{numerator of } f_m) = \deg(\varphi_m^2 \cdot X) = m^2$$

and so the leading coefficient of h_m is $m^2 - 1$.

Now let $x \in K$ be such that $\varphi_{m+1}(x)^2 \cdot \varphi_{m-1}(x)^2 = 0$. Then $P = (x:y:1) \in E(K)$ satisfies $[m\pm1]P = O$, so $[m]P = (x - h_m(x)/\varphi_m(x)^2 : g_m(x)y : 1) = \pm P = (x:\pm y:1) \neq O$ and consequently $\varphi_m(x)^2 \neq 0$ and $h_m(x) = 0$. The polynomial $\varphi_{m+1} \cdot \varphi_{m-1}$ is squarefree since both factors are squarefree so a double root x of it would satisfy $\varphi_{m+1}(x) = \varphi_{m-1}(x) = 0$. This would imply $[m\pm1]P = O$, so $2P = O$ and $F(x) = O$, which is a contradiction since $\varphi_{m+1} \cdot \varphi_{m-1}$ contains at most one factor $X - x$ for $F(x) = 0$. Finally $\deg(\varphi_{m+1} \cdot \varphi_{m-1}) = m^2$ and the leading coefficient is equal to $m^2 - 1$, so the conclusion is that $h_m = \varphi_{m+1}\varphi_{m-1}$.

We now show that $\sqrt{F} \cdot g_m = \varphi_{2m}/(2\varphi_m^4)$. If we write $Fg_m^2 = f_m^3 + a f_m + b$ we see that the denominator of Fg_m^2 is φ_m^6 modulo a unit in K; the numerator and denominator of Fg_m^2 have degrees $3m^2$ and $3(m^2-1)$ respectively; and

$$\frac{\text{leading coefficient numerator of } Fg_m^2}{\text{leading coefficient denominator of } Fg_m^2} = m^{-6}.$$

Let $P = (x:y:1) \in E(K)$ be a point such that $2mP = O$ and $mP \neq O$. Then $yg_m(x) = 0$ which is the case if and only if x is a root of Fg_m^2. It follows that $(\varphi_{2m}/\varphi_m)^2$ is a divisor of the numerator of Fg_m^2 and since these polynomials have the same degree we find

$$g_m\sqrt{F} = \frac{\varphi_{2m}/\varphi_m}{\varphi_m^3} \cdot c.$$

Comparing leading coefficients yields $c = 1/2$. All in all we have shown

$$[m] = \left(X - \frac{\varphi_{m-1}\varphi_{m+1}}{\varphi_m^2} : \frac{\varphi_{2m}/\varphi_m}{2\varphi_m^3} : 1 \right).$$

Any common factor of $\varphi_{m-1}\varphi_{m+1}$ and φ_m^2 comes from a non-zero point $P \in E(K)$ with $mP = [m\pm1]P$ i.e. $\pm P = O$, which is impossible. Clearly φ_{2m}/φ_m and φ_m^3 have no factors in common since we deal with squarefree polynomials. Hence it remains to be shown that $\varphi_m = \psi_m$, from which the result follows since $\psi_{2m}/\psi_m = (\psi_{m+2}(\psi_{m-1})^2 - \psi_{m-2}(\psi_{m+1})^2)/(2\sqrt{F})$ by definition. The equality certainly holds for $m = -1,0,1,2$ and for $m = 3,4$ we can use the representation of $[2]$ found in exercise (4.4). For higher values we use exercise (7.2) applied to $[m]$ and $[n]$, where $m \neq \pm n$ and $mn \neq 0$:

$$\begin{aligned}\varphi_{m+n}\varphi_{m-n} &= \lambda(\varphi_n^2(X\varphi_m^2 - \varphi_{m+1}\varphi_{m-1}) - \varphi_m^2(X\varphi_n^2 - \varphi_{n+1}\varphi_{n-1})) \\ &= \varphi_n^2\varphi_{m+1}\varphi_{m-1} - \varphi_m^2\varphi_{n+1}\varphi_{n-1},\end{aligned}$$

since comparison of leading coefficients yields $\lambda = 1$. So

$$\begin{aligned}\varphi_{2m} &= \varphi_{(m+1)+(m-1)}\varphi_{(m+1)-(m-1)} / 2\sqrt{F} \\ &= ((\varphi_{m-1})^2\varphi_{m+2}\varphi_m - (\varphi_{m+1})^2\varphi_m\varphi_{m-2}) / 2\sqrt{F}\end{aligned}$$

$$= \psi_{2m} ;$$

$$\varphi_{2m+1} = \varphi_{(m+1)+(m)}\varphi_{(m+1)-(m)}$$

$$= \varphi_m{}^2\varphi_{m+2}\varphi_m - (\varphi_{m+1})^2\varphi_{m+1}\varphi_{m-1}$$

$$= \psi_{2m+1} ;$$

by induction. This completes the proof in the case $\text{char}\, K = 0$.

To deal with arbitrary characteristic, first notice that (a) implies (b) in general. We prove (a) by induction on m. Suppose the identity (*) holds over K for $m-1, m$ and $m+1$. Considering φ_m and ψ_m as elements of $\mathbf{Z}[A,B,X,\sqrt{F}]$, then the identity (*) holds for the curve $E = E_{A,B}$ over $\mathbf{Q}(A,B)$ since $\text{char}\, \mathbf{Q}(A,B) = 0$. Hence (*) remains true for $2m$ and $2m+1$, under the ring homomorphism $\mathbf{Z}[A,B] \to K$ taking A to a and B to b, provided $\psi_{2m+1} \neq 0$ and $\psi_{2m} \neq 0$. But $\psi_{2m+1} = 0 \Leftrightarrow \psi_{m+2}(\psi_m)^3 = \psi_{m-1}(\psi_{m+1})^3 \Leftrightarrow X - \psi_m\,\psi_{m+2}/(\psi_{m+1})^2 = X - \psi_{m-1}\psi_{m+1}/\psi_m{}^2$ $\Leftrightarrow [m+1] = \pm[m]$ by induction, which is impossible. In a similar manner we find that $\psi_{2m} \neq 0$, which concludes the proof.

Exercises.

8.1 Show that to calculate ψ_m recursively, one needs to calculate at most $8\cdot 2\log m$ division polynomials of index $\leq m$.

8.2 Let $\{\psi_m \mid m \in \mathbf{Z}_{\geq -1}\}$ be a set of polynomials such that (*) holds for all m. Show that there exists $\lambda \in K^*$ such that $(\psi_m)^2 = \lambda\cdot\prod(X - x_P)^{\deg_i[m]}$ as in the theorem. [Hint: assume K is algebraically closed.]

§9. The structure of the endomorphism ring.

In this section we will have a closer look at the endomorphism ring $\mathrm{End}_K(E)$ of an elliptic curve. As a result we will be able to give the exact number of points of an elliptic curve over a finite field.

(9.1) **Theorem.** Let $R \subset \mathrm{End}_K(E)$ be a commutative subring.
(a) There is an injective ring homomorphism $f: R \to \mathbf{C}$ such that $f(R)$ is a discrete subring of $\mathbf{C}$;
(b) R has an automorphism $\bar{\cdot}$ (*complex conjugation*) of order ≤ 2 ;
(c) For all $r \in R$: $\deg r = r\bar{r}$.

Remark: If $\mathrm{char}\, K = 0$ we can take $R = \mathrm{End}_K(E)$. If $\mathrm{char}\, K = p > 3$ we can take for instance $R = \mathbf{Z}[\mathrm{Frob}_p]$. It can be shown (but this is not easy) that if K is algebraically closed, then $\mathrm{End}_K(E)$ is *not* commutative if and only if E is super-singular. Hence the non-commutative case rarely occurs. See also exercise (9.3).

To prove (9.1) we need a lemma from valuation theory, which we state without proof. The proof is not difficult but lies outside the scope of this text.

(9.2) **Definition.** Let F be a field. An *archimedean valuation* on F is a function $\varphi: F \to \mathbf{R}_{\geq 0}$ satisfying:

(i) $\varphi(x) = 0 \Leftrightarrow x = 0$;
(ii) $\varphi(xy) = \varphi(x)\varphi(y)$;
(iii) $\exists\, C \in \mathbf{R}_{\geq 1}\ \forall\, x,y \in F$: $\varphi(x+y) \leq C \cdot \max\{\varphi(x),\varphi(y)\}$;
(iv) $C = 1$ won't work in (iii) .

Property (iv) is essential. If we can take $C = 1$ the valuation is called *non-archimedean.*

(9.3) **Lemma.** (Ostrowski, Gelfand-Mazur, Tornheim)
Let F be a field and $\varphi: F \to \mathbf{R}$ an archimedean valuation on F. Then there exists an embedding $f: F \to \mathbf{C}$ and a constant $c \in \mathbf{R}_{>0}$ such that $\varphi(x) = |f(x)|^c$.

PROOF: Lang [11, chapter XII] ; Weiss [22, chapter 1] ; Artin [1, chapter 2] or for an analytic proof Rudin [16, chapter 10] .

PROOF of (9.1): Note that R is an integral domain. Let F be the field of fractions of R and define $\varphi(r/s) = \deg(r)/\deg(s)$. By proposition (7.1)

$$\deg(r+s) \leq 2\deg(r) + 2\deg(s) \leq 4 \cdot \max\{\deg(r),\deg(s)\}$$

so φ satisfies properties (i-iii) in (9.2) with $C = 4$, and this is the sharpest value since deg[2] = 4. Hence R can be embedded in $\mathbf{C}$. Moreover we can take $c = 2$, since $4 = \varphi(2) = |f(2)|^c = 2^c$. Hence if $r \in R - \{0\}$ then $|f(r)|^2 \geq 1$, so $f(R)$ is a discrete subring of $\mathbf{C}$. This proves (a), and (b) follows from theorem (6.7). Concerning (c), note that $\deg r = |f(r)|^2 = f(r)\overline{f(r)}$.

(9.4) **Theorem.** Let E be an elliptic curve over $K = \mathbf{F}_q$ and $\varphi = \mathrm{Frob}_q \in \mathrm{End}_K(E)$. Define t_n recursively by $t_0 = 2$, $t = t_1 = \varphi + \overline{\varphi}$, $t_n = tt_{n-1} - qt_{n-2}$. Then

(a) $\varphi^2 - t\varphi + q = 0$;

(b) $|t_n| \leq 2\sqrt{q^n}$;

(c) $\#E(\mathbf{F}_{q^n}) = q^n + 1 - t_n$, $n \geq 1$.

PROOF: (a) See exercise (9.2);

(b) Clear;

(c) In the proof of (7.6) we have seen that $\#E(\mathbf{F}_q) = \deg(\varphi - 1) = (\varphi - 1)(\overline{\varphi - 1}) = |\varphi|^2 - (\varphi + \overline{\varphi}) + 1$. Since $\mathrm{Frob}_{q^n} = \varphi^n$, we have $\#E(\mathbf{F}_{q^n}) = |\varphi|^{2n} - (\varphi^n + \overline{\varphi}^n) + 1$. This gives the required result since by induction $t_n = (\varphi + \overline{\varphi})(\varphi^{n-1} + \overline{\varphi}^{n-1}) - q(\varphi^{n-2} + \overline{\varphi}^{n-2}) = \varphi^n + \overline{\varphi}^n + \varphi\overline{\varphi}(\varphi^{n-2} + \overline{\varphi}^{n-2}) - q(\varphi^{n-2} + \overline{\varphi}^{n-2}) = \varphi^n + \overline{\varphi}^n$.

Exercises.

9.1 (a) For every $\alpha \in \mathrm{End}_K(E)$ there exists a commutative $R \subset \mathrm{End}_K(E)$ containing α, and $\overline{\alpha}$ is independent of the choice of R.

(b) $\overline{\alpha\beta} = \overline{\beta} \cdot \overline{\alpha}$.

(c) $\overline{\alpha + \beta} = \overline{\alpha} + \overline{\beta}$. [Hint: reduce to the case $\alpha = 1$.]

It follows from (b) and (c) that $\bar{\cdot}$ is a *ring anti-automorphism* $R \to R$.

9.2 The *trace* of an endomorphism α is defined as $\mathrm{Tr}(\alpha) = \alpha + \overline{\alpha} \in \mathbf{Z}$.

(a) Prove that $\alpha^2 - \mathrm{Tr}(\alpha)\alpha + \deg(\alpha) = 0$.

(b) Prove that $(\alpha, \beta) = \mathrm{Tr}(\alpha\overline{\beta})$, where $(\cdot,\cdot)$ is the quadratic form defined in §7.

9.3 Suppose $R = \mathrm{End}_K(E)$ is non-commutative. Define an equivalence relation on $R \times \mathbf{Z}_{>0}$ by $(r,n) \sim (s,m)$ iff $rm = sn$ and denote the class of (r,n) by r/n. Let $D = \{\, r/n \mid r \in R$ and $n \in \mathbf{Z}_{>0} \,\}$.

(a) Show that D is a division ring and that $\bar{\cdot}$ and $(\cdot,\cdot)$ can be extended to D.

(b) Show that there exist $\alpha, \beta \in D - \mathbf{Q}$ with $(\alpha,1) = (\beta,1) = (\beta,\alpha) = 0$. Show that any such pair satisfies $\alpha^2, \beta^2 \in \mathbf{Q}_{<0}$ and $\alpha\beta = -\beta\alpha$. [Hint: use Gram-Schmidt orthogonalization.]

(c) If $(\gamma,1) = (\gamma,\alpha) = 0$ then $\gamma \in \mathbf{Q}(\alpha)\cdot\beta$. [Hint: $\mathbf{Q}(\alpha,\gamma/\beta)$ is commutative.]

(d) Conclude that D has a $\mathbf{Q}$-basis $\{1,\alpha,\beta,\alpha\beta\}$ and that the map $D \to \mathbf{H}$ (the quaternions), defined by $\alpha \mapsto \sqrt{|\alpha^2|}i$ and $\beta \mapsto \sqrt{|\beta^2|}j$, embeds R as a discrete subring of $\mathbf{H}$ of rank 4 over $\mathbf{Z}$. Show that the anti-automorphism $\bar{\ }$ is induced by the conjugation on $\mathbf{H}$.

9.4 Let E be an elliptic curve over $\mathbf{F}_q$, where $q = p^k$. Show that E is super-singular $\Leftrightarrow$ for all n, the order of $E(\mathbf{F}_{q^n})$ is not divisible by $p \Leftrightarrow p \mid t = \mathrm{Tr}(\mathrm{Frob}_q)$. If $q = p$ this is the case if and only if $t = 0$.

9.5 In [19, section III.2] it is shown that if E,E' are elliptic curves, then there exists a group homomorphism $\bar{\ }: \mathrm{Hom}_K(E,E') \to \mathrm{Hom}_K(E',E)$ such that

(i) $\varphi\bar{\varphi} = \deg\varphi \in \mathrm{End}_K(E')$;

(ii) $\bar{\varphi}\varphi = \deg\varphi \in \mathrm{End}_K(E)$;

(iii) $\bar{\bar{\varphi}} = \varphi$.

Check that this is true for $K = \mathbf{C}$.

9.6 The *centre* of a ring R is $\mathrm{Z}(R) = \{\, a \in R \mid \forall b \in R : ab = ba \,\}$.

(a) Let E/K be an elliptic curve. If $\mathrm{End}_K E$ is not commutative, then $\mathrm{Z}(\mathrm{End}_K E) = \mathbf{Z}$.

(b) Show that if $K = \mathbf{F}_q$ the Frobenius endomorphism of E/K is in the centre of $\mathrm{End}_K E$.

§10. Counting points on an elliptic curve.

We now have enough theory at hand to describe the algorithms for primality testing and factorization into primes. One sub-algorithm plays an important part, and it deserves special attention: counting the number of points on an elliptic curve over a finite field.

There is one "algorithm" to determine the number of points on an elliptic curve over $\mathbf{F}_q$, which is as trivial as it is useless: count every pair $(x,y) \in \mathbf{F}_q \times \mathbf{F}_q$ which satisfies the equation $y^2 = x^3 + ax + b$, and add one for infinity. This will take q^2 operations. Here (and in the sequel) an *operation* denotes a constant (i.e. independent of q and E) number of additions and multiplications in $\mathbf{F}_q$. Using ordinary methods a multiplication of two numbers of say t digits takes about t^2 time. Using the so called *fast multiplication method* [9], such a multiplication takes $\sim t^{1+\varepsilon}$ time, with $\varepsilon > 0$ arbitrarily small. So we may say that one operation takes $O((\log q)^2)$ time, or $O((\log q)^{1+\varepsilon})$ if we use fast multiplication. The constant in the big O-symbol of Landau depends highly on the speed of your computer.

(10.1) **Proposition.** $\#E(\mathbf{F}_q) = q + 1 + \sum_{x \in \mathbf{F}_q} \chi(x^3 + ax + b)$.

Here $\chi : \mathbf{F}_q \to \{-1,0,1\} \subset \mathbf{Z}$ is the multiplicative character defined by

$$\chi(z) = \begin{cases} -1 \text{ if } z \text{ is not a square in } \mathbf{F}_q; \\ 0 \text{ if } z = 0; \\ 1 \text{ if } z \text{ is a square in } \mathbf{F}_q^*. \end{cases}$$

PROOF: Immediate since $1 + \chi(z) = \#\{ y \in \mathbf{F}_q \mid y^2 = z \}$. The term 1 is for (0:1:0).

Since $\{\chi(z)\}$ is the inverse image of $z^{(q-1)/2}$ under the canonical homomorphism $\mathbf{Z} \to \mathbf{F}_q$, the calculation of $\chi(z)$ takes about $\log q$ squarings. Hence the proposition provides an algorithm taking $q \cdot \log q$ operations.

(10.2) **Algorithm.**

Step 1. Choose a random point $P \in E(\mathbf{F}_q)$.

Step 2. Calculate mP for $q+1-2\sqrt{q} \le m \le q+1+2\sqrt{q}$.

Step 3. If there is a unique m such that $mP = O$ then $m = \#E(\mathbf{F}_q)$ and the algorithm terminates; if there are more than one, then we know the order k of P.

Step 4. Start again by picking $P' \in E(\mathbf{F}_q)$, but now calculate mP' modulo the subgroup generated by P for $(q+1-2\sqrt{q})/k \le m \le (q+1+2\sqrt{q})/k$. We continue in this way for subgroups $\langle P \rangle$, $\langle P,P' \rangle$, $\langle P,P',P'' \rangle$, ..., until the order k of the subgroup that has been found satisfies $|q + 1 - k| \le 2\sqrt{q}$. If $q \ge 37$ then $\#E(\mathbf{F}_q) = k$.

We pick a random point by taking $x \in \mathbf{F}_q$ at random until we find one that satisfies $\chi(x^3 + ax + b) = 1$. It follows from Hasse's theorem (7.6) that about half of the elements of $\mathbf{F}_q$ have this property, so this way of picking points is efficient in a probabilistic sense. We take $P = (x:y:1)$, where y is just a formal symbol. There is an efficient way of calculating square roots in $\mathbf{F}_q$, cf. exercise (10.2).

The calculation of mP for all m will take $O(q^{1/4+\varepsilon})$ operations in $E(\mathbf{F}_q)$, using the so-called *baby step-giant step* method. This method is analogous to an algorithm of Shanks [18] to calculate the class number of an imaginary quadratic number field. The method proceeds as follows. Make a list of all mP for $0 \le m \le q^{1/4}$ (the baby steps), which includes $Q = [q^{1/4}] \cdot P$. (This requires $O(q^{1/4})$ memory, which is not feasible for large q.) Next calculate nQ for $0 < n \le q^{1/4}$ (the giant steps) and check whether $nQ + mP = O$ for mP in the list. This is done by searching the list in $O(\log q)$ time. For any such pair (n,m) we have $(m + [q^{1/4}] \cdot n)P = O$.

To calculate the order of $(P' \bmod P)$ in step 4, we have to compare $m'P'$ wit mP for k values of m and k' values of m', where $kk' = O(\sqrt{q})$. Again this can be done in $O(q^{1/4})$ time using $O(q^{1/4})$ memory using a baby step-giant step strategy. For k small it is clear how this should be done: keep a small list of $<P>$ and walk with baby and giant steps through $<P'>$, comparing with the few values of $<P>$. We can do the same thing with P and P' transposed if k is large. See exercise (10.6). The depth of recursion is $O(\log q)$. In practice it is very small, since most points have a large order.

We see that the expected running time of this algorithm is $O(q^{1/4+\varepsilon})$. In practice it is quite good for q up to 20 decimals. For most elliptic curves a large part of its points have order $> 4\sqrt{q}$. For such a curve a good alternative for step 4 is picking random points on $E(\mathbf{F}_q)$ until one is found of large enough order. Curves that do not have this property exist for instance for $q < 37$ (i.e. $q - [2\sqrt{q}] \le 4\sqrt{q}$) or $q = k^2 + 1$, for which there exist curves with $E(\mathbf{F}_q) \cong \mathbf{Z}/k\mathbf{Z} \times \mathbf{Z}/k\mathbf{Z}$. There is however no good way of telling whether we are dealing with such a curve, so it might happen that this algorithm unfortunately never ends.

For special curves we can calculate $\#E(\mathbf{F}_q)$ very efficiently. Consider for instance the following theorem.

(10.3) **Definition.**

(a) Let $\alpha, \pi \in \mathbf{Z}[i]$ with π prime and $\gcd(2\alpha, \pi) = 1$ and put $q = \pi\overline{\pi}$. The *biquadratic residue symbol* with respect to π is defined as the unique unit of $\mathbf{Z}[i]$ such that:

$$\left(\frac{\alpha}{\pi}\right)_4 \equiv \alpha^{(q-1)/4} \bmod \pi .$$

(b) Let $\alpha,\pi \in \mathbf{Z}[\zeta_3]$ with π prime and $\gcd(6\alpha,\pi) = 1$ and put $q = \pi\overline{\pi}$. The *sixth power residue symbol* with respect to π is defined as the unique unit of $\mathbf{Z}[\zeta_3]$ such that:

$$\left(\frac{\alpha}{\pi}\right)_6 \equiv \alpha^{(q-1)/6} \bmod \pi .$$

(10.4) **Theorem.** Let q be a prime number.

(a) If $q \equiv 1 \pmod 4$ and E is the curve given by $Y^2 = X^3 + aX$ then

$$\#E(\mathbf{F}_q) = (\pi - 1)(\overline{\pi} - 1) ,$$

where $\pi \in \mathbf{Z}[i]$ satisfies $\pi\cdot\overline{\pi} = q$ and $\pi \equiv \left(\frac{-a}{\pi}\right)_4 \pmod{2(1+i)}$.

(b) If $q \equiv 1 \pmod 3$ and E' is the curve given by $Y^2 = X^3 + b$ then

$$\#E'(\mathbf{F}_q) = (\pi - 1)(\overline{\pi} - 1) ,$$

where $\pi \in \mathbf{Z}[\zeta_3]$ satisfies $\pi\cdot\overline{\pi} = q$ and $\pi \equiv \left(\frac{b}{\pi}\right)_6 \pmod{2\sqrt{-3}}$.

Note that in both cases π is unique up to complex conjugation.

PROOF: [8, chapter 18].

The theorem is not surprising if you know that that $\mathrm{End}_{\mathbf{F}_q}(E) \cong \mathbf{Z}[i]$ and $\mathrm{End}_{\mathbf{F}_q}(E') \cong \mathbf{Z}[\zeta_3]$, cf. exercise (6.3), since $\varphi = \mathrm{Frob}_q$ satisfies $\varphi\overline{\varphi} = \deg\varphi = q$ by (9.1) and $(\overline{\varphi}-1)(\varphi-1) = q - (\varphi+\overline{\varphi}) + 1 = \#E(\mathbf{F}_q)$ resp. $\#E'(\mathbf{F}_q)$ by (9.4). However this does not show that π satisfies the congruences stated. For an algorithm to solve $\pi\overline{\pi} = q$ in $\mathbf{Z}[i]$, we refer to exercise (10.3). A similar algorithm can be designed for $\mathbf{Z}[\zeta_3]$.

Another algorithm to calculate $\#E(\mathbf{F}_q)$, due to Schoof, depends on the following theorem.

(10.5) **Theorem.** Let E be an elliptic curve over $\mathbf{F}_q$ and m a positive integer with $\gcd(m,2q) = 1$. Let R be the ring $R = R_m = \mathbf{F}_q[X,Y]/(\psi_m, Y^2 - F)$, where ψ_m is the division polynomial and F the polynomial defining E. Finally let $t = q + 1 - \#E(\mathbf{F}_q)$. Then:

(a) R is a finite ring containing $\mathbf{F}_q$;

(b) $E(R)$ has a group automorphism σ with $\sigma(x:y:z) = (x^q:y^q:z^q)$;

(c) The point $P = (X:Y:1) \in E(R)$ has order m;

(d) $(t \bmod m)$ is characterized by $\sigma^2(P) + qP = t\sigma(P)$.

PROOF: (a) R has an $\mathbf{F}_q$-basis $\{ X^iY^j \mid 0 \le i < (m^2-1)/2 , 0 \le j < 2 \}$, so $\dim_{\mathbf{F}_q} R = m^2 - 1$.

(b) Denote $S = E(\overline{\mathbf{F}_q})[m] - \{O\}$. If $Q = (x_Q:y_Q:1) \in S$ then $\psi_m(x_Q) = 0$ and $y_Q^2 = F(x_Q) \neq 0$

since $2 \nmid m$. It follows that there are ring homomorphisms

$$\phi_Q : R \to \overline{\mathbf{F}_q} \quad , \quad \text{defined by } X \mapsto x_Q \text{ and } Y \mapsto y_Q \ ,$$

and a ring homomorphism

$$\phi : R \to \prod_{Q \in S} \overline{\mathbf{F}_q} \quad , \quad \text{defined by } \phi(r) = (\phi_Q(r))_Q \ .$$

If $g,h \in \mathbf{F}_q[X]$ are such that $\phi(g+hY) = 0$, then for all $Q \in S$ we have $g(x_Q) \pm h(x_Q)y_Q = 0$ and since $y_Q \neq 0$ this means that $g(x_Q) = h(x_Q) = 0$ and hence $\psi_m \mid g$ and h. This shows that ϕ is injective and by exercise (2.6) we may consider $E(R)$ as a subgroup of $\prod_{Q \in S} E(\overline{\mathbf{F}_q})$ by means of the embedding ϕ_*. Since $\mathbf{F}_q \subset R$, the map $x \mapsto x^q$ is a ring endomorphism of R. So we can define $\sigma : E(R) \to E(R)$ by $\sigma(x:y:z) = (x^q:y^q:z^q)$. The restriction of σ to each coordinate is the Frobenius morphism on $E(\overline{\mathbf{F}_q})$, which is bijective, so σ is an injective group homomorphism and hence an automorphism since R is finite.

(c) By definition $\phi_*(P) = (Q)_{Q \in S}$. Each coordinate has an order which is a divisor of m and by corollary (7.3a) at least one coordinate has order exactly m.

(d) Denote $\varphi = \mathrm{Frob}_q$. By theorem (9.4) $\varphi^2 - t\varphi + q = 0$, in particular $\varphi^2(Q) - t\varphi(Q) + qQ = O$ and hence $\sigma^2(P) - t\sigma(P) + qP = O$. Since P has order m and σ is an automorphism, any number t satisfying this equation is determined modulo m.

(10.6) **Algorithm.**

Step 1. Determine the smallest x such that $\prod_{p \text{ prime}, p \leq x, \gcd(p,2q)=1} p \ > \ 4\sqrt{q}$.

Step 2. Calculate ψ_m for $m \leq x$.

Step 3. Calculate $(t \bmod p)$ for every p prime, $p \leq x$, $\gcd(p,2q)=1$, using the theorem.

Step 4. Calculate $(t \bmod \prod p)$ using the Chinese remainder theorem. Then t is uniquely determined by $|t| \leq 4\sqrt{q}$, and $\#E(\mathbf{F}_q) = q + 1 - t$.

The speed of this algorithm depends mainly on the size of x. We claim that $x = O(\log q)$. This is clear from the *prime number theorem* [6], which states that

$$\sum_{p \text{ prime}, p \leq x} \log p \ \sim \ x \ ,$$

but it also follows from exercise (10.5).

To calculate $(t \bmod p)$ in step 3, we first calculate $\sigma^2 P + qP$ in $O(\log q)$ arithmetic operations in the ring $R = R_p$. Next we calculate $0 \cdot \sigma P$, $1 \cdot \sigma P$, $2 \cdot \sigma P$,... until we find $t \cdot \sigma P = \sigma^2 P + qP$. This will take at most p operations in R. Since R has dimension p^2-1 over $\mathbf{F}_q$, one arithmetic operation in R takes $O(p^4)$ operations in $\mathbf{F}_q$. We may say that the number of primes $p \leq x$ is $\sim \log q$. In fact this number is $O(x/\log x)$, so this is a reasonable estimation. Furthermore we may take $p \sim \log q$ which is reasonable for a large part of the p. So step 3 takes

$$\begin{aligned} &(\text{number of } p) \cdot (O(\log q) + O(\log q)) \text{ operations in } R \\ = \ &O((\log q) \cdot (\log q + \log q) \cdot (\log q)^4) \ = \ O((\log q)^6) \text{ operations in } \mathbf{F}_q \ . \end{aligned}$$

The calculation of ψ_m takes $\log(m)$ multiplications of polynomials of degree $\sim m^2-1$, so step 2 takes $O((\log q)^5)$ operations in $\mathbf{F}_q$. We conclude that Schoof's algorithm takes $O((\log q)^8)$ time using conventional multiplication. Fast multiplication methods can perform a multiplication in R_p using $O(p^{2+\varepsilon})$ multiplications in $\mathbf{F}_q$, so the algorithm takes $O((\log q)^{5+\varepsilon})$ time using fast multiplication.

Exercises.

10.1 Let $G = <\varphi>$ be the multiplicative group generated by $\varphi = \mathrm{Frob}_q \in \mathrm{Aut}(E(\mathbf{F}_q))$ and let S be as in theorem (10.5). Choose a set of representatives Σ for the orbits of $Q \in S$ under the action of G. Show that:

(a) $R \cong \prod_{Q \in \Sigma} \mathbf{F}_q(x_Q, y_Q)$;

(b) $[\mathbf{F}_q(x_Q, y_Q) : \mathbf{F}_q] = \#\{ \varphi^i Q \mid i \in \mathbf{Z} \}$.

10.2 Let q be an odd prime power and denote $q - 1 = 2^k \cdot u$ with $k,u \in \mathbf{Z}$ and u odd. Let $r \in \mathbf{F}_q$ satisfy $r^{2^{k-1}} = -1$. Such an element exists and is easy to find, for instance $r = s^u$, with $\chi(s) = -1$, where χ is the character defined in (10.1). Finally let $a \in \mathbf{F}_q$ with $\chi(a) = 1$. Prove the correctness of the following algorithm to solve $x^2 = a$ in $\mathbf{F}_q$.

(1) Let $x = a^{(u+1)/2}$ and $c = a^u$.

(2) If $c = 1$ then $x^2 = a$ and the algorithm terminates.

(3) If not, then determine the smallest positive integer m such that $c^{2^m} = 1$.
Replace x by $x \cdot r^{2^{k-1-m}}$ and c by $c \cdot r^{2^{k-m}}$ and go back to step 2.
[Hint: show that $x^2 = ac$ always holds, and eventually $c = 1$.]

10.3 Let p be a prime number, $p \equiv 1 \bmod 4$. Suppose $x \in \mathbf{Z}$ satisfies $x^2 \equiv -1 \bmod p$. Such an x can be found as in (10.2). Define $f : \mathbf{Z}[i] \to \mathbf{F}_p$ by $f(c + di) = (c + dx \bmod p)$.

(a) Prove that f is a ring homomorphism and $\ker f$ is generated by p and $x - i$.

(b) Show that $\ker f = \mathbf{Z}[i] \cdot \pi$ where $\pi = a + bi \in \mathbf{Z}[i]$ satisfies $\pi\overline{\pi} = p$.

(c) Show that $xb \equiv -a \bmod p$.

(d) Prove that π can be found by calculating the greatest common divisor of p and $x - i$ in $\mathbf{Z}[i]$ using the Euclidean algorithm.

Remark: A faster method to find such a number π, or rather to find $a,b \in \mathbf{Z}$ satisfying $a^2 + b^2 = p$, is the following [3]. Let again $x \in \mathbf{Z}$ satisfy $x^2 \equiv -1 \bmod p$. We may assume $0 < x < p$. Now define $r_0, r_1, \ldots$ by

$r_0 = p$, $r_1 = x$,

$r_{n-1} = q_n r_n + r_{n+1}$, $0 < r_{n+1} < r_n$.

The algorithm terminates when $r_n < \sqrt{p}$, and then $p = r_n^2 + r_{n+1}^2$.

10.4 Prove the *Chinese remainder theorem* for $\mathbf{Z}$:

Let $n_1 , \ldots , n_t$ be pairwise coprime positive integers, i.e. $\gcd(n_i,n_j) = 1$ for $1 \le i < j \le t$. Then $\mathbf{Z}/(\prod n_i)\mathbf{Z} \cong (\mathbf{Z}/n_1\mathbf{Z}) \times \ldots \times (\mathbf{Z}/n_t\mathbf{Z})$. Furthermore for every t-tuple of integers $(a_1,\ldots,a_t)$ there exists an integer a , such that $a \equiv a_i \bmod n_i$ for $1 \le i \le t$. This a is uniquely determined modulo $\prod n_i$.

10.5 (a) Show that every prime power that divides $\binom{n}{k}$ is $\le n$.

(b) $2^n = \sum_{k=0}^{n} \binom{n}{k} \le (n+1)\cdot n^{\sqrt{n}} \cdot \prod_{p \text{ prime}, p \le n} p$.

(c) There exists $c > 1$ such that for all $n \ge 2$: $\prod_{p \text{ prime}, p \le n} p \ge c^n$.

(d) $\prod_{p \text{ prime}, \lceil n/2 \rceil < p \le n} p \le \binom{n}{[n/2]} \le 2^n$.

(e) There exists $d > 1$ such that for all $n \ge 1$: $\prod_{p \text{ prime}, p \le n} p \le d^n$.

(Note: $[n/2]$ denotes the greatest integer $\le n/2$ and $\lceil n/2 \rceil$ denotes the smallest integer $\ge n/2$.)

10.6 Let $P,P' \in E(\mathbf{F}_q)$ with $\text{order}(P) = k \le 4\sqrt{q}$. Let $S = [(q+1)/k]P'$.

(a) There exists k' with $|kk'| \le 2\sqrt{q}$ and $kP + k'P' = S$.

Assume that $k \le 2q^{1/4}$ and let $Q = [2q^{1/4}]P'$.

(b) Show that one can calculate *all* triples (m,m',n) such that

$$mP + m'P' + nQ = S \quad \text{and} \quad |m| \le k \, , \, |m'| \le 2q^{1/4} \, , \, |n| \le 2q^{1/4}/k$$

in $O(q^{1/4})$ time using $O(q^{1/4})$ memory.

(c) Show that this can be used to calculate the order of $(P' \bmod P)$, and it gives the order of $E(\mathbf{F}_q)$ if there is only one such triple.

(d) Show that a similar method works for $k > 2q^{1/4}$.

*(e) Generalize this to calculate $k_{t+1} = \text{order}(P_{t+1} \bmod \langle P_1 , \ldots , P_t \rangle)$ from

$k_i = \text{order}(P_i \bmod \langle P_1 , \ldots , P_{i-1} \rangle)$, $1 \le i \le t$.

§11. Primality proving.

Although it is not hard to convince yourself of the primality of a given number n, it is quite hard to give a sound mathematical proof of this. In this section we will show how the theory of elliptic curves can be applied to design a primality proving algorithm. It should be noted that there exist fast so-called *pseudo-primality tests*, such as the one outlined in exercise (11.1), which give an almost certain answer to the question whether a number is prime or not. In fact it seems less likely that a number passing a reasonable pseudo-primality test is *not* prime, than that your computer equipment has been wrecked by some species of vermin, or even that in the future someone will find a logical paradox in the foundations of mathematics which will turn all the results in these notes into false statements anyway.

(11.1) **Theorem.** Let n be an integer greater than 1, not divisible by 2 or 3. Suppose there exists an elliptic curve E over $\mathbf{Z}/n\mathbf{Z}$ and $m, q \in \mathbf{Z}_{>0}$ and $P \in E(\mathbf{Z}/n\mathbf{Z})$ such that:
(i) q is a prime divisor of m and $q > (n^{1/4} + 1)^2$;
(ii) $mP = O$ in $E(\mathbf{Z}/n\mathbf{Z})$;
(iii) If $[m/q]P = (x:y:z)$ then $z \in (\mathbf{Z}/n\mathbf{Z})^*$.
Then n is prime.

PROOF: Let p be a prime divisor of n. The canonical homomorphism $\mathbf{Z}/n\mathbf{Z} \to \mathbf{Z}/p\mathbf{Z}$ induces a homomorphism $E(\mathbf{Z}/n\mathbf{Z}) \to E(\mathbf{Z}/p\mathbf{Z})$ which maps $[m/q]P$ to $Q = (x:y:z)$. Now $Q \neq O$, since $\mathbf{Z}/p\mathbf{Z}$ is a field and $z \in (\mathbf{Z}/p\mathbf{Z})^*$ by (iii). It follows from (i) and (ii) that

$$(n^{1/4} + 1)^2 < q = \text{order of } Q \text{ in } E(\mathbf{Z}/p\mathbf{Z}) \leq \#E(\mathbf{Z}/p\mathbf{Z}) \leq (\sqrt{p} + 1)^2,$$

so $p > \sqrt{n}$ and hence $p = n$.

Let $n \in \mathbf{Z}_{>1}$, $\gcd(n,6) = 1$. If n is prime, the following algorithm provides a proof of this. However, if n is not prime there is no certainty that the algorithm will tell you so (although it will do for "most" numbers). In the algorithm we use an undefined constant C, which influences the speed of the algorithm and whose size depends on n. It should be chosen such that given a random number $m \approx n$, the probability that m has *exactly* one prime factor $\geq C$ is large, and the time needed to find *all* prime factors $< C$ of m is short. We call a number *probably prime* if it has passed a pseudo-primality test.

(11.2) **Algorithm.** Let $n \in \mathbf{Z}_{>1}$, $\gcd(n,6) = 1$. We determine whether n is prime as follows:
Step 1. Subject n to a pseudo-primality test such as in exercise (11.1), and terminate if n is not prime.
Step 2. Choose an elliptic curve over $\mathbf{Z}/n\mathbf{Z}$ and $m \in \mathbf{Z}_{>0}$ such that

if n is prime **then** $m = \#E(\mathbf{Z}/n\mathbf{Z})$.

If $m \notin [n+1-2\sqrt{n}, n+1+2\sqrt{n}]$ then n is not prime and the algorithm terminates.

Step 3. Let k be the product of all prime factors of m smaller than C, and denote $q = m/k$. Now check if

(i) $k > 1$;

(ii) $q > (n^{1/4} + 1)^2$;

(iii) q is probably prime.

If one of these properties does not hold, go back to step 2.

Step 4. Choose a random $P = (x:y:1) \in E(\mathbf{Z}/n\mathbf{Z})$. Proceed until we find a point P such that $kP = (x':y':z') \neq O$. If $\gcd(z',n) \neq 1$ then n is not prime and the algorithm terminates.

Step 5. If $mP \neq O$ then n is not prime and the algorithm terminates. If $mP = O$ all the assumptions of theorem (11.1) are satisfied, except possibly that q is prime.

Step 6. Prove recursively that q is prime.

Step 1 needs no explanation. There are two methods to choose E and m in step 2, which are treated separately in (11.3) and (11.7). To find small prime factors of m in step 3 we can use for instance the algorithm described in the next section. The probability that m has only large prime factors (i.e. $k = 1$) or that it has only small prime factors (i.e. $q \leq (n^{1/4} + 1)^2$) is quite small, at least in comparison to the probability that q is not prime, which is $\sim 1 - 1/\log n$ by the prime number theorem. So the probability that (i), (ii) and (iii) are satisfied is probably $O(1/\log n)$ and hence we can expect that step 2 (which is the most time-consuming part of the algorithm) must be repeated $O(\log n)$ times at each recursive step.

In step 4 a point P is found by picking x at random such that $(x^3 + ax + b)^{(n-1)/2} \equiv 1 \bmod n$ and solving $y^2 \equiv x^3 + ax + b \bmod n$ as in exercise (10.2). This algorithm is efficient in a probabilistic sense if n is prime. If n is not prime the algorithm either provides a good solution, or it ends up telling you that n is not prime (for instance if it finds s such that $s^{(n-1)/2} \not\equiv -1, 0 \text{ or } 1 \bmod n$), or it may have trouble finding an s with $s^{(n-1)/2} \not\equiv 0 \text{ or } 1 \bmod n$. So if no such s is found after a few tries, it is best to terminate the whole algorithm and reconsider your suspicion that n is prime. You might try another pseudo-primality test, or even try it the other way around: decompose n into irreducible factors, e.g. by the algorithm in the next section.

We calculate multiples of P by repeatedly doubling. We can use the doubling formula of exercise (4.4), which also works over $\mathbf{Z}/n\mathbf{Z}$. If n is prime the probability that $kP \neq O$ is $(q-1)/q$, see exercise (11.2).

Since $q \leq (n + 2\sqrt{n} + 1)/2 \approx n/2$, the depth of recursion is bounded by $c \cdot \log n$. Note that if q is below a certain bound it is better to apply more direct methods to prove the primality of q. The expected running time is $O((\log n)^2)$·the time taken by step 2, which yields a total time of $O((\log n)^{10})$ if we use the Goldwasser-Kilian method, or $O((\log n)^{6+\varepsilon})$ using Atkin's method.

(11.3) **First method to choose E and m.** (Goldwasser-Kilian).

Step 1. Choose $0 \leq a,b < n$ arbitrarily, until $4a^3 + 27b^2 \not\equiv 0 \bmod n$.

Step 2. Check whether $\gcd(4a^3 + 27b^2, n) = 1$. If this is not the case we have found a non-trivial divisor of n and we can finish the job.

Step 3. Calculate m using Schoof's algorithm (10.6).

Note that Schoof's algorithm only works in the case that n is prime, but if this is not the case any number m, even the one provided by Schoof, satisfies the condition of step 2 in (11.2). It is however quite likely that in that case Schoof's algorithm will terminate by telling that n is not prime.

The second method, due to Atkin, is in a way reverse to the first, since it starts by calculating m, and then tries to find an elliptic curve E with $\#E(\mathbf{Z}/n\mathbf{Z}) = m$ (if n is prime). Since the construction of E is the hard part of Atkin's method, we must of course first check if m is of the desired magnitude and that it has a probably prime divisor q satisfying the conditions in step 3 of (11.2). Before describing the algorithm, we state a few facts.

(11.5) **Definition.** Let $p \geq 5$ be a prime number. The *complex multiplication field* of an elliptic curve E over the prime field $\mathbf{F}_p$ is defined to be $L = \mathbf{Q}(\sqrt{d})$, where $d = t^2 - 4p$ with $t \in \mathbf{Z}$ such that $\#E(\mathbf{F}_p) = p + 1 - t$.
The *ring of integers* of L is $O_L = \{ x \in L \mid \exists f \in \mathbf{Z}[X]$ monic such that $f(x) = 0 \}$.

A complex multiplication field is an *imaginary quadratic field*, since $d < 0$. It is an elementary fact from algebraic number theory that an imaginary quadratic field is of the form $L = \mathbf{Q}(\sqrt{\Delta})$, with Δ a negative integer not divisible by the square of an odd prime, and $\Delta \equiv 1 \bmod 4$ or $\Delta \equiv 8$ or $12 \bmod 16$. This number Δ is called the *discriminant* of L. The ring of integers of such an L is $O_L = \mathbf{Z}[(\Delta + \sqrt{\Delta})/2]$.

(11.6) **Theorem.** Let $L = \mathbf{Q}(\sqrt{\Delta})$ be an imaginary quadratic field. Then there exists a monic irreducible polynomial $F_L \in \mathbf{Z}[X]$ such that for all primes $p \nmid 6\Delta$, for which $\pi\overline{\pi} = p$ is solvable in O_L, the following properties hold:

(a) $\overline{F_L} = (F_L \bmod p)$ splits into distinct linear factors over $\mathbf{F}_p$.

(b) If $j \in \mathbf{F}_p$ is a zero of $\overline{F_L}$, then every elliptic curve $E/\mathbf{F}_p$ with $j(E) = j$ has L as its complex multiplication field.

The degree of F_L is equal to h_L, the class number of O_L.

PROOF: See [21], where it is also shown how to construct these polynomials. In [17] one can find a few useful remarks on how long this will take.

It is easy to determine whether $\pi\overline{\pi} = p$ is solvable in O_L, and indeed to solve it, by methods analogous to those indicated in exercise (10.3) for $O_L = \mathbf{Z}[i]$, i.e. $\Delta = -4$. The solution π is unique up to conjugation and multiplication by units.

(11.7) **Second method to choose E and m.** (Atkin).

Step 1. Select $\Delta \in \{-3,-4,-7,-8,-11,-15,-19,-20,...\}$ with $\gcd(\Delta,n) = 1$, for which $\pi\overline{\pi} = n$ is solvable in the ring of integers O_L of the field $L = \mathbf{Q}(\sqrt{\Delta})$, and solve it.

Step 2. Calculate $m = (\pi - 1)(\overline{\pi} - 1)$.

Step 3. Find $j \in \mathbf{F}_p$ with $\overline{F_L}(j) = 0$.

Step 4. Find an elliptic curve with $j(E) = j$ and $\#E(\mathbf{Z}/n\mathbf{Z}) = m$ if n is prime.

By exercise (3.2) there are 6 (if $j = 0$), 4 (if $j = 1728$) or 2 (otherwise) isomorphism classes of elliptic curves with $j(E) = j$ and by exercise (11.3) there are 6 (if $\Delta = -3$), 4 (if $\Delta = -4$) or 2 (if $\Delta \leq -7$) possible values of m. It can be shown that if $\Delta \neq -3,-4$ then 0 an 1728 are not zeros of F_L, and $F_{\mathbf{Q}(\sqrt{-3})} = X$ resp. $F_{\mathbf{Q}(i)} = X - 1728$. So given j with $\overline{F_L}(j) = 0$, there is a bijective correspondence between possible values of m and isomorphism classes of elliptic curves with $j(E) = j$. For $\Delta = -3,-4$ it is easy to match the right curve with the right m, using theorem (10.4), since all the curves with $j(E) = 0,1728$ are of the form $E = E_{0,b}$ or $E_{a,0}$ respectively. For $\Delta \leq -7$ two non-isomorphic curves with j-invariant j are for instance $E = E_{3k,2k}$ and $E' = E_{3kc^2,2kc^3}$, where $k = j/(1728 - j)$ and $c^{(n-1)/2} \equiv -1 \bmod n$ (provided n is prime). There may be good ways to find out which curve has the right order, but these are not known. The best way seems to be to choose arbitrary points on them until one is found which is not annihilated by m. In that case the other curve must have order m.

Rather than calculating the polynomial F_L we keep a list of all of them for the first few hundred discriminants. This should be enough if $n \approx 10^{200}$, which is about the size of a number that the elliptic-curve-method-primality-proving-machine can handle effectively. Zeros of F_L can be easily found using general zero-finding routines over finite fields [9, section 4.6.2].

It is hard to give an exact analysis of the time needed by this algorithm. A heuristic analysis shows, modulo some unproved assumptions, that given Δ, we can find m in $O((\log n)^{3+\varepsilon})$ time [13]. Since calculating F_L is hard it should be checked first whether m satisfies the properties in steps 2 and 3 of the main algorithm. A good value of m can be found in probably $O((\log n)^{2+\varepsilon})$ time. Once we've got m, calculating E will cost $O((\log n)^{5+\varepsilon})$ time. Note that the degree of F_L not too large by the Brauer-Siegel theorem. So Atkin's method takes $O((\log n)^{5+\varepsilon})$ time, and with recursion

the whole algorithm takes $O((\log n)^{6+\varepsilon})$ time.

Exercises.

11.1 Let $n > 1$ be an odd number, say $n - 1 = u \cdot 2^t$, with u odd and $t \geq 1$.

(a) If n is prime, then every $a \in (\mathbf{Z}/n\mathbf{Z})-\{0\}$ satisfies:
$a^u = 1$ or $-1 \in \{ a^u, a^{2u}, \ldots, a^{2^{t-1} \cdot u} \}$. (*)

*(b) If n is *not* prime then (*) holds for at most 25% of all $a \in (\mathbf{Z}/n\mathbf{Z})-\{0\}$.

(c) Let $r \in \mathbf{Z}$ with $r \equiv 2 \bmod 4$, such that $p = r + 1$ and $q = 2r + 1$ are prime. Let $n = pq$. Show that $\#\{ a \in \mathbf{Z}/n\mathbf{Z} \mid a^{(n-1)/2} = \pm 1\} = \#\{ a \in \mathbf{Z}/n\mathbf{Z} \mid a$ satisfies (*) $\} = r^2/2$.

It is conjectured that there exist infinitely many $r \in \mathbf{Z}$ as in (c). It follows that the bound in (b) is sharp in the sense that there exists a sequence (n_k) of non-primes such that $\#\{ a \in \mathbf{Z}/n_k\mathbf{Z} \mid a$ satisfies (*) $\} \sim n_k/4$ asymptotically if $k \to \infty$. Also for $n = 9$ we have exactly 25% in (b).

11.2 Let n,m,k,q be as in algorithm (11.2) and assume that n is prime. Show that $\#E(\mathbf{Z}/n\mathbf{Z})[k] = k$. [Hint: $\gcd(k,q) = 1$.]

11.3 Let L an imaginary quadratic field of discriminant Δ. Show that:

(a) The ring of integers O_L of L is a discrete subring of $\mathbf{C}$.

(b) The discriminant of O_L, as defined in (6.10), is equal to Δ.

(c) $O_L^* = \begin{cases} \{ \pm 1, (\pm 1 \pm \sqrt{-3})/2 \} & \text{if } \Delta = -3; \\ \{ \pm 1, \pm i \} & \text{if } \Delta = -4; \\ \{ \pm 1 \} & \text{otherwise.} \end{cases}$

§12. Factoring integers.

In contrast to primality testing, the difficulty of the factorization of an integer into primes lies in obtaining the answer. The verification that the answer is correct is completely trivial. We first give an older algorithm, for its striking analogy with the elliptic curve algorithm. As before, n is a positive integer.

(12.1) **Algorithm.** ($p-1$ - method, Pollard 1974)

Step 1. Choose a number k that is composed of small primes, e.g. $k = \text{kgv}(1,2,...,C)$, for some constant C.

Step 2. Choose $a \bmod n$ arbitrary.

Step 3. Calculate $d = \gcd(a^k - 1, n)$.

Step 4. If $1 < d < n$ we have found a non-trivial divisor of n. If $d = 1$ start again, putting some more primes into k. If $d = n$, try again with another a or take some primes out of k.

If p is a prime factor of n with $p-1 \mid k$ then $p \mid \gcd(a^k-1,n)$, since by Fermat's theorem p divides $a^{p-1}-1$. Hence the method works if n has a prime factor p such that $p-1$ is completely built up from small primes. If this is not the case the method is not likely to work.

We calculate $a^k-1 \pmod n$ in $O(\log k)$ squarings and multiplications mod n. The running time is $O((\log n)^2 \cdot C)$.

The following method differs from Pollard's method in that it uses the structure of the group $E(\mathbf{F}_p)$ instead of the multiplicative group $(\mathbf{Z}/p\mathbf{Z})^*$. The advantage of this lies in the fact that if one curve doesn't work we can always try another. Let n be non-prime, $\gcd(n,6) = 1$ (factors 2 and 3 can be easily found) and not a power. This can be checked by calculating $n^{1/2}, n^{1/3}, \ldots, n^{1/k}$ for $k = [^2\log n]$. There are two parameters v and w in the algorithm. The constant v is an upper bound for the size of the prime factor we want to find. We can take $v = [\sqrt{n}]$, but since the speed of the algorithm depends highly on v it is better to choose v smaller. The other constant w depends on v and we shall see below how it can be calculated.

(12.2) **Algorithm.**

Step 1. Choose an elliptic curve E over $\mathbf{Z}/n\mathbf{Z}$ and $P = (x:y:1) \in E(\mathbf{Z}/n\mathbf{Z})$.

Step 2. Let $e(r) = \max\{e \in \mathbf{Z}_{\geq 0} \mid r^e \leq (\sqrt{v} + 1)^2\}$ and let

$$k = \prod_{r \text{ prime}, r \leq w} r^{e(r)}.$$

Calculate successively for $i = 0,1,2 \ldots, \sum e(r)$:

k_i = (product of the i smallest primes in k) and $P_i = k_i P = (x_i:y_i:z_i)$;
until we have found the largest i (which is $\leq \sum e(r)$) with $z_i \not\equiv 0 \bmod n$.

Step 3. Calculate $d = \gcd(z_i , n)$, which is divisor of n that is strictly smaller than n . If $d = 1$ start again at step 1.

The best way to choose E and P is to choose arbitrary (a,x,y) and take $b = y^2 - x^3 - ax$, until we find $\gcd(4a^3 + 27b^2,n) \not\equiv 0 \bmod n$. If gcd > 1 we have found a non-trivial divisor of n . If gcd =1 we take $E = E_{a,b}$ and $P = (x:y:1)$. Step 2 takes

$\sum_r \{e(r)$ multiplications-by-$r\}$ in $E(\mathbf{Z}/n\mathbf{Z})$ =
$O(\sum e(r)\log r)$ operations in $\mathbf{Z}/n\mathbf{Z}$ =
$O(\sum \log r^{e(r)})$ operations in $\mathbf{Z}/n\mathbf{Z}$ =
$O(w\cdot\log v)$ operations in $\mathbf{Z}/n\mathbf{Z}$ =
$O(w\cdot\log v\cdot(\log n)^2)$ time.

To analyse the algorithm we need to know the probability that a random triple (a,x,y) provides a pair (E,P) that gives a non-trivial divisor. A sufficient condition for (E,P) to do so is given in the following theorem.

(12.3) **Theorem.** Let n, v and w be as above and let E be an elliptic curve over $\mathbf{Z}/n\mathbf{Z}$ with $P = (x:y:1) \in E(\mathbf{Z}/n\mathbf{Z})$. Suppose n has prime divisors p and q such that:
(i) $p \leq v$;
(ii) $\#E(\mathbf{F}_p)$ is composed of primes $\leq w$;
(iii) $\#E(\mathbf{F}_q)$ is not divisible by the largest prime factor of the order of $(P \bmod p) \in E(\mathbf{F}_p)$.
Then the algorithm (12.2) finds a non-trivial divisor of n .

PROOF: Let r be a prime number with $r^m \mid \#E(\mathbf{F}_p) \leq (\sqrt{p} + 1)^2 \leq (\sqrt{v} + 1)^2$. It follows from (ii) that $r \leq w$ and by definition $m \leq e(r)$. Hence $\#E(\mathbf{F}_p) \mid k$. Now suppose the algorithm doesn't find a non-trivial divisor, then there exists $i \leq \sum e(r)$ with

$\gcd(z_i,n) = 1$ and $\{ i = \sum e(r)$ (*) or $z_{i+1} = 0$ (**) $\}$.

It is impossible that (*) holds, since in that case $k = k_i$ and $k\cdot(P \bmod p) = (kP \bmod p) = (O \bmod p)$ so $p \mid z_i$ and hence $\gcd(z_i,n) > 1$. Also (**) is impossible since this would imply $p,q \mid z_{i+1}$ and

$k_i\cdot(P \bmod p,q) \neq (O \bmod p,q)$ (since p and q are prime) ;
$k_{i+1}\cdot(P \bmod p,q) = (O \bmod p,q)$.

If $k_{i+1} = rk_i$ then it would follow that r is the largest prime divisor of the order of $(P \bmod p,q)$, which is in contradiction with condition (iii).

The following theorem shows how the orders of elliptic curves over $\mathbf{F}_p$ are distributed over the

interval $(p+1-2\sqrt{p}, p+1+2\sqrt{p})$.

(12.4) **Theorem.** Let $p > 3$ be a prime.

(a) Let E be an elliptic curve over $\mathbf{F}_p$. Then $\operatorname{End} E = \operatorname{End}_{\mathbf{F}_p} E$ is a discrete subring of $\mathbf{C}$ not equal to $\mathbf{Z}$.

(b) Let $t \in \mathbf{Z}$ with $|t| \le 2\sqrt{p}$ and R a discrete subring of $\mathbf{C}$. Then

$$\#\{E/\mathbf{F}_p \mid \#E(\mathbf{F}_p) = p+1-t \ , \operatorname{End} E \cong R \}/\cong_{\mathbf{F}_p} \ = \begin{cases} h_R \text{ if } R \text{ contains a zero of } X^2-tX+p \ , \\ 0 \text{ otherwise} . \end{cases}$$

PROOF: (a) Let $\varphi = \operatorname{Frob}_p \in \operatorname{End} E$. Since $|\varphi| = \sqrt{p}$ we can't have $\operatorname{End} E \cong \mathbf{Z}$. Moreover exercise (9.6) shows that $\varphi \in Z(\operatorname{End} E) = \{ \psi \in \operatorname{End} E \mid \forall \chi : \chi\psi = \psi\chi \}$ and that $Z(\operatorname{End} E) = \mathbf{Z}$ if $\operatorname{End} E$ is not commutative.

(b) See [5]. Note that this is analogous to theorem (6.11).

(12.5) **Corollary.** Let E be an elliptic curve over $\mathbf{F}_p$ and $t \in \mathbf{Z}$ with $|t| \le 2\sqrt{p}$. Then

$$N_t \ = \ \#\{E/\mathbf{F}_p \mid \#E(\mathbf{F}_p) = p+1-t \ \}/\cong \ = \ |t^2-4p|^{1/2+o(1)} \text{ for } p \to \infty .$$

PROOF: Comparing discriminants we see that $X^2 - tX + p$ is solvable in R if and only if

$$t^2 - 4p \ = \ d^2 \cdot \Delta_R .$$

By the Brauer-Siegel theorem $h_R = |\Delta_R|^{1/2+o(1)}$. So

$$N_t \ = \ \sum_{d^2 \mid t^2-4p} |(t^2-4p)/d^2|^{1/2+o(1)} \ = \ |t^2-4p|^{1/2+o(1)} \text{ for } p \to \infty .$$

We now sketch how to find an upper bound for the number N of triples $(\alpha,\xi,\eta) \in (\mathbf{Z}/n\mathbf{Z})^3$ for which the algorithm provides a non-trivial divisor. Details can be found in [14]. Keep v and w fixed and assume that n has a prime divisor $p \le w$. To simplify the analysis, we assume $|t| \le \sqrt{p}$, i.e. we consider only a part of the possible choices of (E,P). In real life the probability that a random pair will work can only be greater. Let S be the set

$$S = \{ t \in \mathbf{Z} \mid |t| \le \sqrt{p} \text{ and } p+1-t \text{ is completely built up of primes} \le w \} .$$

If $|t| \le \sqrt{p}$, then $|t^2-4p|^{1/2} \approx \sqrt{p}$ and it can be shown that the $o(1)$ in (12.5) doesn't vary too much with t, in fact for $|t| \le \sqrt{p}$ there exists a constant c_1 such that $c_1 / \log p \ \le \ |t^2-4p|^{o(1)}$ for all t with the possible exception of one $|t|$. So for all but possibly two $t \in S$ we have

$$N_t \ \ge \ c_1 \sqrt{p} / \log p \ . \qquad (1)$$

The number of curves $E_{a,b}/\mathbf{F}_p$ of order $p+1-t$ (up to isomorphism) with $(x:y:1) \in E_{a,b}(\mathbf{F}_p)$ is N_t. Furthermore there are $(p-1)/\#\operatorname{Aut} E \ge c_2 \cdot (p-1)$ isomorphic curves, and $p-t$ affine points on a curve of order t. So

$$\#\{\ (a,b,x,y) \in (\mathbf{Z}/p\mathbf{Z})^4 \mid 4a^3 + 27b^2 \neq 0\ ,\ \#E_{a,b}(\mathbf{F}_p) \in S$$
$$\text{and } (x{:}y{:}1) \in E_{a,b}(\mathbf{F}_p) \qquad \} \ \geq$$

$$\sum_{t\in S} N_t \cdot (p-1)(p-t)/\#\mathrm{Aut}\ E \ \geq\ c_3\cdot(\#S-2)\cdot p^{5/2} / \log p\ . \tag{2}$$

Denote for $t \in S$:

$$T_t = \{\ (a,x,y) \in (\mathbf{Z}/p\mathbf{Z})^3 \mid 4a^3 + 27b^2 \neq 0\ ,$$
$$\#E_{a,b}(\mathbf{F}_p) = p + 1 - t \quad \text{for } b = y^2 - x^3 - ax\ \}\ ;$$

and for $(a,x,y) \in T_t$:

$$r_{axy} = \text{largest prime dividing the order of } (x{:}y{:}1) \in E_{a,b}(\mathbf{F}_p)\ ,$$
$$U_{axy} = \{\ (a',x',y') \in (\mathbf{Z}/q\mathbf{Z})^3 \mid 4a'^3 + 27b'^2 \neq 0\ ,$$
$$\#E_{a',b'}(\mathbf{F}_p) \text{ is not divisible by } r_{axy}\ \},$$

where $b' = y'^2 - x'^3 - a'x'$. It can be shown that if q and r are primes, $q > 3$, then

$$\#\{E/\mathbf{F}_q \mid \#E(\mathbf{F}_q) \not\equiv 0 \bmod r\ \}/\cong\ \geq\ c_4\cdot q\ >\ 0, \tag{3}$$

so $\#\,U_{axy} \geq c_5\cdot q^3$. Theorem (12.3) implies that

$$N \geq \sum_{t\in S} \sum_{(a,x,y)\in T_t} \sum_{(a',x',y')\in U_{axy}} \#V_{axya'x'y'} \tag{4}$$

where

$$V_{axya'x'y'} = \{\ (\alpha,\xi,\eta) \in (\mathbf{Z}/n\mathbf{Z})^3 \mid (\alpha \bmod p, \xi \bmod p, \eta \bmod p) = (a,x,y) \text{ and}$$
$$(\alpha \bmod q, \xi \bmod q, \eta \bmod q) = (a',x',y')\ \}\ .$$

It is clear that $\#V_{axya'x'y'} = n^3 / (pq)^3$ and combining (1), (2), (3) and (4) we obtain

$$N / n^3\ \geq\ c_6\textstyle\sum_t \#T_t / p^3\ \geq\ c_6(\sum_{t\in S} \#T_t)/p^3\ \geq\ c_7(\#S-2)\ /\ \sqrt{p}(\log p)\ , \tag{5}$$

where N / n^3 is the probability that a random triple is succesful in the algorithm. Now let $f(w) = \#S\ /\ ([2\sqrt{p}] + 1)$ be the probabilitity that a random integer t in the interval $(-\sqrt{p}, \sqrt{p})$ is in S . If $\#S > 2$ we can rewrite (5) as

$$N / n^3\ \geq\ c_8 f(w) / \log p\ \geq\ c_8 f(w) / \log v\ . \tag{6}$$

We now have established the following proposition.

(12.6) **Proposition.** Let n, v and w be as in (12.2) and suppose n has a prime divisor $p \leq v$. Let $f(w)$ be the probability that a random integer in the interval $(p+1-\sqrt{p}, p+1+\sqrt{p})$ is completely built up from primes $\leq w$. Then the algorithm finds a non-trivial divisor of n in an expected time

$$O(w(\log v)(\log n)^2 f(w)^{-1}(\log v))\ ,$$

provided $f(w) \geq 3\ /\ (\ [2\sqrt{p}] + 1\ )$.

To make the algorithm as efficient as possible we have to choose w such that $w/f(w)$ is as small

as possible. To establish this, we introduce another function $g(w)$ = probability that a random number in the interval $(1, p)$ is completely built up from primes $\leq w$. Then $g(w) = \psi(p,w)/p$, where $\psi(x,y) : \mathbf{Z}_{>0} \times \mathbf{Z}_{>0} \to \mathbf{Z}_{>0}$ is defined by

$$\psi(x,y) = \#\{\, a \in \mathbf{Z} \mid 1 \leq a \leq x \text{ and } a \text{ is completely built up from primes} \leq y \,\}.$$

This function is called the *Dickman-de Bruijn* function.

(12.6) **Theorem.** Let $\varepsilon > 0$. If $x \geq 10$ and $y > (\log x)^{1+\varepsilon}$, then

$$\psi(x,y) = x \cdot u^{-u+o(u)} \text{ uniformly for } u \to \infty,$$

where $u = \log y / \log x$.

PROOF: [4, theorem 3.1].

If $g(w) = \psi(p,w)/p$, then

$g(w)$ = probability that a random number in the interval $(1, p)$ is completely built up from primes $\leq w$.

It follows from the theorem that $g(w) \sim u^{-u}$, for $u = \log w / \log p$, and that if

$$w = e^{\sqrt{(\log p)(\log \log p)/2}\cdot(1+o(1))}$$

then so is $g(w)^{-1}$. This suggests a choice for w. Since p is not known beforehand, we should replace p by v. If we assume that $f(w) \approx g(w)$, which seems a reasonable conjecture, the running time of the algorithm is

$$O(e^{\sqrt{2(\log p)(\log \log p)}\cdot(1+o(1))}\cdot(\log v)^2(\log n)^2) =$$
$$O(e^{\sqrt{2(\log v)(\log \log v)}\cdot(1+o(1))}\cdot(\log n)^2).$$

We have a worst case bound if n is a product of two primes of the same order of magnitude. In that case $v \approx \sqrt{n}$ and the running time is $O(e^{\sqrt{(\log n)(\log \log n)}\cdot(1+o(1))})$. This running time has also been proposed for other factoring methods such as the class group method and the quadratic sieve method. The present method has the advantage that the running time depends on the size of the smallest prime factor of n. Therefore it is particularly suitable for factoring integers with a relatively small prime factor. However in view of applications such as cryptography, these numbers are not the most interesting. Another advantage of algorithm (12.2) is that it needs very little storage: it requires $O(\log n)$ memory, which is about the room needed to store the number n.

References.

1. E. Artin, *Algebraic numbers and algebraic functions*, Gordon and Breach, New York 1967.

2. I.G. Bashmakova, *Diofant i diofantovii uravnienia*, Nauka, Moscow 1972; German translation: *Diophant und diophantische Gleichungen*, Deutscher Verlag der Wissenschaften, Berlin 1974.

3. J. Brillhart, *Note on representing a prime as a sum of two squares*, Math. of Computation **26** (1972), 1011-1013.

4. E.R. Canfield, P. Erdös, C. Pomerance, *On a problem of Oppenheim concerning "Factorisatio Numerorum"*, J. Number Theory **17** (1983), 1-28.

5. M. Deuring, *Die Typen der Multiplikatorenringe elliptischer Funktionenkörper*, Abh. Math. Sem. Hansischen Univ. **14** (1941), 197-272.

6. G.H. Hardy & E.M. Wright, *An introduction to the theory of numbers*, fifth edition, Oxford University Press, Oxford 1979.

7. R. Hartshorne, *Algebraic geometry*, Graduate Texts in Math. **52**, Springer Verlag, New York 1977.

7a. D. Husemöller, *Elliptic curves*, Graduate Texts in Math. **111**, Springer Verlag, New York 1987.

8. K. Ireland & M. Rosen, *A classical introduction to modern number theory*, Graduate Texts in Math. **84**, Springer Verlag, New York 1982.

9. D.E. Knuth, *The art of computer programming*, vol. 2, *Seminumerical algorithms*, second edition, Addison-Wesley, Reading, Mass. 1981.

10. N. Koblitz, *Introduction to elliptic curves and modular forms*, Graduate Texts in Math. **97**, Springer Verlag, New York 1984.

11. S. Lang, *Algebra*, second edition, Addison-Wesley, Reading, Mass. 1980.

12. S. Lang, *Algebraic number theory*, Addison-Wesley, Reading, Mass. 1970.

13. A.K. Lenstra & H.W. Lenstra, Jr., *Algorithms in number theory*, in: J. van Leeuwen (ed.), *Handbook of theoretical computer science*, North-Holland, Amsterdam, to appear.

14. H.W. Lenstra, Jr., *Factoring integers with elliptic curves*, report 86-18, Mathematisch Instituut, Universiteit van Amsterdam 1986; Ann. of Math., to appear.

15. H.W. Lenstra, Jr., *Elliptic curves and number-theoretic algorithms*, report 86-19, Mathematisch Instituut, Universiteit van Amsterdam 1986; Proceedings International Congress 1986, Berkeley, to appear.

16. W. Rudin, *Functional Analysis*, McGraw-Hill, New York 1973.

17. R.J. Schoof, *Elliptic curves over finite fields and the computation of square roots mod p*, Math. Comp. **43** (1985), 483-494.

18. D. Shanks, *Class number, a theory of factorization, and genera*, pp. 415-440 in: Proc. Symp. Pure Math. **20** (1969 Institute on number theory), Amer. Math. Soc., Providence 1971.

19. J.H. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Math. **106**, Springer Verlag, New York 1986.

20. J. Tate, *The arithmetic of elliptic curves*, Invent. Math. **23** (1974), 179-206.

21. H. Weber, *Lehrbuch der Algebra*, vol. III, Friedrich Vieweg und Sohn, Braunschweig 1908; reprint: Chelsea Publishing Company, New York.

22. E. Weiss, *Algebraic number theory*, McGraw-Hill, New York 1963; reprint Chelsea Publishing Company, New York 1976.

Index.

APPENDIX TO

Elliptic Curves and Factorization Algorithms.

§1. The class group.

Throughout this section, K denotes a field of charactaristic $\neq 2$ (hence char $K = 3$ is allowed), $F \in K[X]$ is a monic polynomial of degree $2g + 1$, where g is a positive integer. There is a factorization $F = F_0 \cdot F_1^2$, where F_0 is squarefree, i.e. F_0 is not divisible by the square of an irreducible element in $K[X]$. Note that $F_0 \notin K$ since F has odd degree. We have an extension of rings

$$\begin{array}{ccc} K(X) & \subset & K(X,\sqrt{F}) \\ \cup & & \cup \\ K[X] & \subset & K[X,\sqrt{F}] \ . \end{array}$$

(1.1) **Definition.** Let R be a ring (commutative with 1 as always). An *R-module* is an abelian group M together with a pairing $R \times M \to M$, $(r,m) \mapsto r \cdot m$ that satisfies the following axioms:

(M1) $(r + s)m = rm + sm$;
(M2) $r(m + n) = rm + rn$;
(M3) $r(sm) = (rs)m$;
(M4) $1 \cdot m = m$.

with $r,s \in R$ and $m,n \in M$.

If R is a field then an R-module is the same as a vector space. Every abelian group A is a $\mathbf{Z}$-module in a canonical way, by defining $n \cdot a = a + \ldots + a$ (n times). Ideals of R are R-modules with the usual addition and multiplication. A ring homomorphism $f : R \to S$ induces an R-module structure on the additive group S by defining $r \cdot s = f(r)s$.

An R-module M is called *finitely generated* if there exist $m_1, \ldots, m_k \in M$ such that every element $m \in M$ can be written as $m = \sum r_i m_i$ with $r_i \in R$.

(1.2) **Definition.** An *order in* $K(X,\sqrt{F})$ is a subring $A \subset K(X,\sqrt{F})$ such that
(i) $K[X] \subset A$;
(ii) A is a finitely generated $K[X]$-module.
(iii) The field of fractions of A is $Q(A) = K(X,\sqrt{F})$;

(1.3) **Proposition.** Let $M \subset K(X,\sqrt{F})$ be a finitely generated $K[X]$-module, which generates

$K(X,\sqrt{F})$ as a vector space over $K(X)$.

(a) There exist $p,q,r \in K(X)$, with $p,r \neq 0$, such that

$$M = K[X]\cdot p + K[X]\cdot(q + r\sqrt{F}) .$$

(b) M is an order if and only if there exists $f \in K[X]-\{0\}$ such that

$$M = K[X] + K[X]\cdot f\sqrt{F_0} .$$

(c) There is a bijection

$$\{f \in K[X] \text{ monic } \} \to \{ \text{ orders in } K(X,\sqrt{F}) \}$$

defined by

$$f \mapsto K[X,f\sqrt{F_0}] .$$

PROOF: (a) After multiplying M by a common multiple of the denominators of the generators of M we may assume $M \subset K[X,\sqrt{F}]$. Define $\pi : M \to K[X]$ by $a + b\sqrt{F} \to b$. The image of π is a submodule of $K[X]$ which is non-trivial since M generates $K(X,\sqrt{F})$ over $K(X)$. Such a module is an ideal in $K[X]$, and since $K[X]$ is a principal ideal domain, $\pi(M) = K[X]r$, with $r \in K[X]-\{0\}$. It follows that there exists $q \in K[X]$ with $q + r\sqrt{F} \in M$. If $\alpha,\beta \in M$ form a basis of $K(X,\sqrt{F})$ over $K(X)$ then $0 \neq \pi(\beta)\alpha - \pi(\alpha)\beta \in \ker(\pi)$, so the kernel of π is a non-trivial submodule of $K[X]$, hence

$$\ker(\pi) = M \cap K[X] = K[X]p ,$$

with $p \in K[X]-\{0\}$. It is clear that $K[X]p + K[X](q+r\sqrt{F}) \subset M$. On the other hand, if $a + b\sqrt{F} \in M$ then $b = b_1 r \in K[X]r$. Since $b_1(q + r\sqrt{F}) \in M$ we have

$$a - b_1 q = (a+b\sqrt{F}) - b_1(q+r\sqrt{F}) \in M \cap K[X] = K[X]p$$

and

$$a + b\sqrt{F} = (a-b_1 q) + b_1(q+r\sqrt{F}) \in K[X]p + K[X](q+r\sqrt{F}) .$$

(b) Clearly a module of the form $K[X]+K[X]f\sqrt{F_0} = K(X,f\sqrt{F_0})$ with $f \neq 0$ is an order in $K(X,\sqrt{F})$. Conversely, suppose $M = K[X]p + K[X](q+r\sqrt{F})$, with $p,q,r \in K(X)$ is a subring of $K(X,\sqrt{F})$. Then 1 and p^2 are elements of $M \cap K(X) = K[X]p$. Hence p^{-1} and $p \in K[X]$, i.e. $p \in K[X]^*$. This shows

$$M = K[X] + K[X]\gamma$$

with $\gamma = q+r\sqrt{F}$. On the one hand we can write

$$\gamma^2 = a + b\gamma$$

with $a,b \in K[X]$. On the other hand, the minimum polynomial of γ over $K(X)$ is $T^2 - 2qT + (q^2-r^2F)$, so

$$\gamma^2 = (r^2F-q^2) + 2q\gamma .$$

Since 1 and γ are linearly independent over $K(X)$ we see that $q = b/2 \in K[X]$ and hence $(rF_1)^2F_0 = r^2F = a + q^2 \in K[X]$. It follows that the denominator of $(rF_1)^2$ is squarefree, since F_0 is squarefree. In other words

$f =_{\text{def}} rF_1 \in K[X]$.

Since $f\sqrt{F_0} = r\sqrt{F} = \gamma - q$ this shows

$$M = K[X] + K[X]\gamma = (K[X] + K[X]q) + K[X](\gamma - q) = K[X] + K[X]f\sqrt{F_0}\,.$$

(c) Immediate from (b). |||

(1.4) **Definition.** Let A be an order in $K(X,\sqrt{F})$. A subset $M \subset K(X,\sqrt{F})$ is called an *invertible A-module* if it is an A-module and if there there exists an A-module $M' \subset K(X,\sqrt{F})$ such that $M\cdot M' = A$, where $M\cdot M'$ is the A-module generated by $\{xy \mid x \in M\,,\, y \in M'\}$. An invertible A-module of the form αA , with $\alpha \in K(X,\sqrt{F})^*$, is called *principal.*

It is obvious that the invertible A-modules form a multiplicative abelian group I_A with unit element A . In particular the inverse M' of M is uniquely determined. From $MM' = A$ we see that there exist $x_i \in M$ and $y_i \in M'$, $1 \le i \le k$, such that $\sum x_i y_i = 1$. Hence the module $Ax_1 + \ldots + Ax_k$ coincides with M since they have the same inverse M' . This shows that M is finitely generated over A and that for some $\alpha \in A$ the $K[X]$-module αM satisfies the conditions of (1.3). The principal modules form a subgroup P_A of I_A . The qoutient group $Cl_A = I_A/P_A$ is called the *class group* of A. Two invertible modules M and N that are in the same coset of P_A are called *equivalent*, denoted $M \sim N$.

Let $M = \alpha(K[X] + K[X]\gamma)$, with $\alpha,\gamma \in K(X,\sqrt{F})^*$ and $\gamma \notin K(X)$. Then γ is quadratic over $K(X)$, so there exist $a,b,c \in K[X]$ with $\gcd(a,b,c) = 1$ and $a \neq 0$, such that $a\gamma^2 - b\gamma + c = 0$.

(1.5) **Proposition.** Under the assumptions above, M is an invertible $K[X,\sqrt{F}]$-module if and only if $b^2 - 4ac \in (K^*)^2 \cdot F$.

PROOF: Let σ be the automorphism of order 2 of $K(X,\sqrt{F})$ sending $p + q\sqrt{F}$ to $p - q\sqrt{F}$. Then $\gamma\sigma(\gamma) = c/a$ and $\gamma + \sigma(\gamma) = b/a$. Hence

$$\begin{aligned} M\cdot\sigma(M) &= \alpha\sigma(\alpha)\cdot\big(K[X] + \gamma K[X] + \sigma(\gamma)K[X] + \gamma\sigma(\gamma)K[X]\big) \\ &= \alpha\sigma(\alpha)\cdot\big(K[X] + \gamma K[X] + b/aK[X] + c/aK[X]\big) \\ &= a^{-1}\cdot\alpha\sigma(\alpha)\cdot\big(aK[X] + a\gamma K[X] + bK[X] + cK[X]\big) \\ &= a^{-1}\cdot\alpha\sigma(\alpha)\cdot\big(K[X] + a\gamma K[X]\big)\,, \end{aligned}$$

since $aK[X] + bK[X] + cK[X] = K[X]$. Hence M is an invertible $K[X,a\gamma]$-module, with inverse $a\sigma(M)/\alpha\sigma(\alpha)$. By exercise (1.1) M is an invertible $K[X,\sqrt{F}]$-module if and only if $K[X,\sqrt{F}] = K[X,a\gamma] = K[X,\sqrt{b^2 - 4ac}]$. By proposition (1.3.c) this is possible if and only if $\sqrt{F}$ is equal to $\sqrt{b^2 - 4ac}$ up to unit of K . |||

(1.6) **Theorem.** Let $H = H_F$ be the set

$$H = \{\, (a,b,c) \in K[X]^3 \mid \begin{array}{l} \gcd(a,b,c) = 1, \\ a \text{ monic}, \\ \deg b < \deg a \le g, \\ b^2 - 4ac = 4F \end{array} \,\},$$

and let

$$\varphi(a,b,c) = \frac{b/2 + \sqrt{F}}{a} \in K(X,\sqrt{F}),$$

for $(a,b,c) \in H$. Then there is a bijection $H \to Cl = Cl_{K[X,\sqrt{F}]}$ defined by

$$(a,b,c) \mapsto \text{class of } K[X] + K[X]\cdot\varphi(a,b,c).$$

PROOF: There is an embedding of $K(X,\sqrt{F})$ into $K((t))$ defined by

$$X \mapsto t^{-2} + \dots,$$
$$\sqrt{F} \mapsto t^{-2g-1} + \dots,$$

cf. (I.5.2). Let $d : K(X,\sqrt{F}) \to K((t)) \to \mathbf{Z} \cup \{\infty\}$ be given by the composition of this embedding with the degree function $\deg_t(\sum a_i t^i) = \inf\{\, i \mid a_i \neq 0 \,\}$. Let $\gamma = \varphi(a,b,c)$ and $M = K[X]+K[X]\gamma$. The properties of the degree function derived in exercise (I.5.2) imply $d\gamma = -(2g+1) + 2\deg a \le -1$, and for $p,q \in K[X]$

$$d(p+q\gamma) = \min\{\, -2\deg p, -2\deg q + d\gamma \,\}.$$

(With the convention that $\deg 0 = -\infty$.) It follows that

$$\{\, y \in M \mid dy = \max\{dx \mid x \in M - \{0\}\} \,\} = K^*. \tag{1}$$

and

$$\{\, y \in M \mid dy = \max\{dx \mid x \in M - K[X]\} \,\} = \{\, p \in K[X] \mid \deg p \le g - \deg a \,\} + \gamma K^*. \tag{2}$$

Suppose $\gamma = \varphi(a',b',c')$ and $M' = K[X]+K[X]\gamma$ is equivalent to M, say $M = \alpha M'$. It follows from (1) that $d\alpha = 0$. Hence $\alpha \in K^*$ and $M = M'$. Now it follows from (2) that $\deg a = \deg a'$ and

$$\gamma = \lambda\gamma + p, \tag{3}$$

for $p \in K[X]$ and $\lambda \in K^*$. If we compare the $\sqrt{F}$-coordinates of both expressions in (3) we find that $a = \lambda a'$ and since a,a' are monic $\lambda = 1$ and $a = a'$. The equality (3) now reduces to

$$b'/2 = pa + b/2.$$

But since $\deg a > \deg b$ and $\deg a > \deg b'$ this can only be an equality if $p = 0$. This proves that the map $H \to Cl$ is injective.

Conversely, let M be an invertible module. Multiplying M by a suitable element of $K(X,\sqrt{F})$ if necessary, we may assume $M \subset K[X,\sqrt{F}]$ and $\max\{dx \mid x \in M - \{0\}\} = 0$. By proposition (1.3.a) there exist $p \in K[X]$ and $\gamma \in K[X,\sqrt{F}]$ such that $M = K[X]p + K[X]\gamma$. Note that

$$d\gamma = d(q+r\sqrt{F}) \leq -(2\deg r + 2g + 1) < 0$$

since $r \neq 0$. It follows that $dp = \max\{dx \mid x \in M-\{0\}\} = 0$, so $p \in K^*$ and

$$M = K[X] + K[X]\gamma.$$

Let $a,b,c \in K[X]$ be such that $\gcd(a,b,c) = 1$, a is monic and $a\gamma^2-b\gamma+c = 0$. We will modify (γ,a,b,c) step by step, without changing M, until $(a,b,c) \in H$ and $\varphi(a,b,c) = \gamma$. By proposition (1.5) there exist $\lambda \in K^*$ such that $b^2-4ac = \lambda^2 F$. Replacing γ by $2\lambda^{-1}\gamma$ we obtain $a(2\lambda^{-1}\gamma)^2 - (2\lambda^{-1}b)(2\lambda^{-1}\gamma) + 4\lambda^{-2}c = 0$ and $(2\lambda^{-1}b)^2 - 4a(4\lambda^{-2}c) = 4F$, so we may assume $\lambda^2 = 4$. It remains to be shown that $\deg b < \deg a \leq g$. One easily verifies that the quadruple

$$(\gamma+q,\ a,\ b+2aq,\ c + bq - aq^2)$$

satisfies the same properties as (γ,a,b,c) above and that in addition $\deg b+2aq < \deg a$ for a suitable value of q. Hence we may assume $\deg b < \deg a$. Furthermore

$$0 > d\gamma = d(b'/2 \pm \sqrt{F}) - da = \min\{db, d\sqrt{F}\} - da.$$

Since $db > da$ we must have $da > d\sqrt{F} = -2g-1$, i.e. $\deg a \leq g$. We now have achieved that $(a,b,c) \in H$ and $\varphi(a,b,c) = \pm\gamma$. But then $\varphi(a,\pm b,c) = \gamma$ and M is in the image of the map $H \to Cl$. |||

(1.7) Definition. A Weierstrass-curve is a triple $E=(a_2,a_4,a_6) \in K^3$. The set of points of E over a field extension $L \supset K$ is

$$E(L) = \{ (x:y:z) \in \mathbb{P}^2(L) \mid y^2z = x^3 + a_2x^2z + a_4xz^2 + a_6z^3 \}.$$

A K-isomorphism $E \to E'$ is a pair $(u,a) \in K^* \times K$ such that

$$u^2 a_2 = 3a + a_2',$$
$$u^4 a_4 = 3a^2 + 2aa_2' + a_4',$$
$$u^6 a_6 = a^3 + a^2a_2' + aa_4' + a_6'.$$

Note that an isomorphism induces a bijection between the sets of points $E(L)$ and $E'(L)$, given by $(0:1:0) \mapsto (0:1:0)$ and $(x:y:1) \mapsto (u^2x+a : u^3y : 1)$, since

$$(u^3y)^2 = (u^2x)^3 + u^2a_2(u^2x)^2 + u^4a_4u^2x + u^6a_6$$
$$= (u^2x+a)^3 + a_2'(u^2x+a)^2 + a_4'(u^2x+a) + u^6a_6.$$

A point $P=(x:y:z) \in E(L)$ is called singular if the partial derivatives G_X, G_Y and G_Z of the polynomial

$$G = Y^2Z - X^3 - a_2X^2Z - a_4XZ^2 - a_6Z^3$$

vanish simultaneously in (x,y,z). This does not depend on a particular representation of P since G is homogeneous. The point $O=(0:1:0)$ is never singular, since $G_Z(0,1,0) = 1$. Let $F = X^3 + a_2X^2 + a_4X + a_6$ be the defining polynomial of $E=(a_2,a_4,a_6)$. If $(x:y:1) \in E(L)$ is singular then $G_Y(x,y,1) = 2y = 0$ hence $y^2 = F(x) = 0$ and $G_X(x,y,1) = F_X(x) = 0$. We see that the singular points of $E(L)$ are in one-to-one correspondence with the double zeros of F in L. Since $\deg F = 3$ the set of points contains at most one singular point. The set of non-singular points of $E(L)$ is denoted by $E_{ns}(L)$. A Weierstrass curve is called non-singular if $E_{ns}(\bar{K}) = E(\bar{K})$, or equivalently if the discriminant $\Delta(f) \neq 0$. Consequently the non-singularity of a Weierstrass curve only depends on its isomorphism class, for if $E \cong E'$ then the defining polynomial F' is obtained from F by linear substitution

If $\operatorname{char} K \neq 3$ a Weierstrass curve (a_2,a_4,a_6) is isomorphic to $(0, a_4 - a_2^2/3, a_6 - 4a_2^5/27 - a_2a_4/3)$ via the isomorphism $(1, a_2/3)$. Hence in this case we can identify the isomorphism classes of elliptic curves with the isomorphism-classes of non-singular Weierstrass curves. In particular two elliptic curves are isomor-

phic as in the sense of definition (I.1.2) if and only if they are isomorphic as Weierstrass curves.

(1.8) Definition. Let E be a Weierstrass curve over K, and $P,Q \in E(K)$. The sum $P+Q$ is defined as follows:

(i) If P (or Q) $= \mathcal{O}$ then $P+Q = Q$ (or P).

(ii) If $P=(x_1:y_1:1)$ and $Q=(x_2:y_2:1)$ then

$P+Q = \mathcal{O}$ if $x_1=x_2$ and $y_1=-y_2$

and

$$P+Q = (x_3 : -(\lambda x_3 + r) : 1),$$

with

$$\lambda = \frac{y_2-y_1}{x_2-x_1} \quad \text{or} \quad \lambda = \frac{x_1^2 + x_1x_2 + x_2^2 + a_2(x_2+x_1) + a_4}{y_2+y_1},$$

$$r = y_1 - \lambda x_1$$

and

$$x_3 = \lambda^2 - x_1 - x_2 - a_2,$$

otherwise.

Clearly this definitions extends definition (I.1.3). In particula the three points $(x_i:y_i:1)$ for $i=1,2,3$ in the „generic" case (with $y_3 = \lambda x_3 + r$) are the three intersection points of the line $y=\lambda x+r$ with the affine part of the Weierstrass points

(1.9) Theorem. Let E be a Weierstrass curve over K with defining polynomial F. Then there is a bijection

$$E_{ns}(K) \longrightarrow H_F$$

defined by

$$(0:1:0) \longmapsto (1,0,-F)$$

$$(x:y:1) \longmapsto (X-x, -2y, \frac{y^2-F}{X-x}),$$

such that the composed map $\varphi : E_{ns}(K) \longrightarrow H_F \longrightarrow \mathcal{O}_E := \mathcal{O}_{K[X,\sqrt{F}]}$ satisfies $\varphi(P+Q) = \varphi(P)\cdot\varphi(Q)$.

The important corollary of this theorem is

(1.10) Corollary. The addition in (1.8) defines a group law on $E_{ns}(K)$, and $\tilde{E}_{ns}(K) \cong \mathcal{O}_E^*$. In particular the addition law for elliptic curves defined in (I.1.3) induces an abelian

group structure on $E(K)$. □

Before proving the theorem we shall have a closer look at the case that E is singular. The situation is as follows.

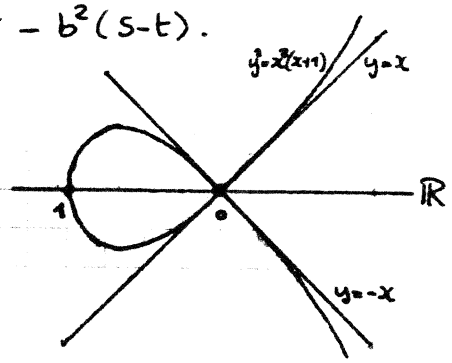
If $F = (X-s)^2(X-t)$ and $s \neq t$ then the singularity $S = (s:0:1)$ is called a node. It is straightforward that $s, t \in K$, by exercise (1.4). Apart from $x=s$, the lines through S are given by $y = \alpha(x-s)$, $\alpha \in \bar{K}$. The intersection points of this line with $E(\bar{K})$ are given by the zeros of $\alpha^2(X-s)^2 - (X-s)^2(X-t)$. A line through S is tangent to $E(\bar{K})$ if this polynomial has one triple zero, s, hence if $\alpha^2 = s-t$. There is a map

$$E_{ns}(K) \longrightarrow K(\sqrt{s-t})$$

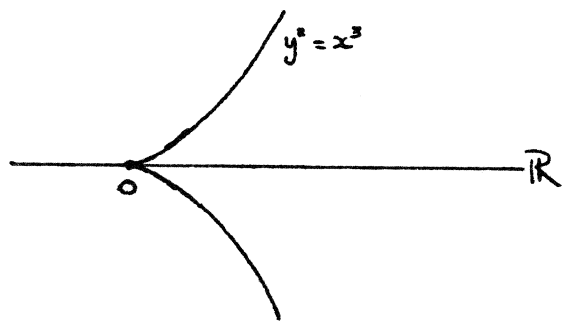
defined by

$$O \longmapsto 1,$$
$$(x:y:1) \longmapsto \frac{y - \sqrt{s-t}(x-s)}{y + \sqrt{s-t}(x-s)} \neq 1.$$

If the tangents at S are rational, i.e. $\sqrt{s-t} \in K$, then this map is an isomorphism $E_{ns}(K) \cong K^*$. If the tangents are quadratic, i.e. $\sqrt{s-t} \notin K$, then $E_{ns}(K)$ is isomorphic to the group of elements of norm 1 in $K(\sqrt{s-t})$ where the norm of an element is $N(a+b\sqrt{s-t}) = a^2 - b^2(s-t)$.



NODE



CUSP

If $F = (X-s)^3$ then the singularity is called a cusp. Clearly $s \in K$ if $\mathrm{char}\, K \neq 3$ or if K is perfect (a field of characteristic p is called perfect if $p=0$, or $p>0$ and $s^p \in K \Leftrightarrow s \in K$ for all $s \in \bar{K}$). In this case $E_{ns}(K)$ is isomorphic to the additive group K^+ via the map

$$O \longmapsto 0,$$
$$P = (x:y:1) \longmapsto \frac{y}{x-s} = \frac{1}{\text{slope } PS}.$$

PROOF OF (1.9): It is easy to see that the map $E_{ns}(K) \to H_F$ is well defined and bijective. In particular $X-x \mid y^2-F$ since $F(x)=y^2$. For the composition φ we have

$$(0:1:0) \longmapsto (1,0,-F) \longmapsto \text{class of } K[X]+K[X]\sqrt{F} = K[X,\sqrt{F}]$$

$$(x:y:1) \longmapsto (X-x,-2y,\dots) \longmapsto \text{class of } K[X]+K[X]\frac{-y+\sqrt{F}}{X-x} \sim K[X](X-x)+K[X](\sqrt{F}-y).$$

It remains to be shown that φ respects addition. Let $P,Q \in E_{ns}(K)$. If $O \in \{P,Q\}$ then $\varphi(P+Q)=\varphi(P)\cdot\varphi(Q)$ since $\varphi(O)=K[X,\sqrt{F}]$ is the unit element of Cl_E.

If $P=-Q=(x:y:1)$ then

$$\varphi(P)\cdot\varphi(Q) = \big(K[X](X-x)+K[X](\sqrt{F}-y)\big)\cdot\big(K[X](X-x)+K[X](\sqrt{F}+y)\big).$$

We have to show that this is a principal ideal in $K[X,\sqrt{F}]$. In fact we shall show that is equal to $K[X,\sqrt{F}](X-x)$.

The inclusion $\varphi(P)\varphi(Q) \subset K[X,\sqrt{F}](X-x)$ is clear since $X-x \mid (\sqrt{F}-y)(\sqrt{F}+y)$.

Conversely if $y \neq 0$ then

$$X-x = \frac{1}{4y}\big((X-x)+(\sqrt{F}+y)\big)\big((X-x)-(\sqrt{F}-y)\big) - \frac{1}{4y}\big((X-x)-(\sqrt{F}+y)\big)\cdot\big((X-x)+(\sqrt{F}-y)\big).$$

If $y=0$ then $F=f\cdot(X-x)$ with f and $X-x$ coprime since x is not a double zero of F, and hence $1=\lambda f+\mu(X-x)$ for some $\lambda,\mu \in K[X]$, and

$$X-x = \lambda F + \mu(X-x)^2 \in \big(K[X](X-x)+K[X]\sqrt{F}\big)^2 = \varphi(P)\varphi(Q).$$

This proves the case $P=-Q$.

Let $O \neq P \neq -Q \neq O$, say $P=(x_1:y_1:1)$ and $Q=(x_2:y_2:1)$. Put

$$x_3 = \lambda^2 - x_1 - x_2 - a_2$$

and

$$y_3 = \lambda x_3 + r,$$

where λ, r have (one of) the values in (1.8). Since we have already shown that $\varphi(O)=1$ and $\varphi(-P)=\varphi(P)^{-1}$ it is sufficient to show that

$$\prod_{i=1}^{3}\big(K[X](X-x_i)+K[X](\sqrt{F}-y_i)\big) = K[X,\sqrt{F}]\cdot(\sqrt{F}-\lambda X-r).$$

As we have seen $y_i=\lambda x_i+r$, so the left expression equals

$$I := \prod_{i=1}^{3}\big(K[X](X-x_i)+K[X](\sqrt{F}-\lambda X-r)\big).$$

The inclusion $I \subset K[X,\sqrt{F}]\cdot(\sqrt{F}-\lambda X-r)$ now follows from the fact that

$$\prod_{i=1}^{3}(X-x_i) = F-(\lambda X+r)^2 = (\sqrt{F}+\lambda X+r)(\sqrt{F}-\lambda X-r) \in K[X,\sqrt{F}](\sqrt{F}-\lambda X-r).$$

The other inclusion is clear if the x_i are pairwise distinct, for in that case there exist $\lambda_i \in K[X]$ such that

$$\lambda_3(X-x_1)(X-x_2)+\lambda_2(X-x_1)(X-x_3)+\lambda_1(X-x_2)(X-x_3) = 1$$

and

$$\sqrt{F}-\lambda X-r = \sum_{i=1}^{3}\Big(\lambda_i(\sqrt{F}-\lambda X-r)\cdot\prod_{j\neq i}(X-x_j)\Big) \in I.$$

Finally suppose the x_i are not distinct, say $\xi = x_i = x_j$ for some $i \neq j$. Let J be the $K[X, \sqrt{F}]$- ideal

$$J = \{ f \in K[X, \sqrt{F}] \mid f \cdot (\sqrt{F} - \lambda X - \nu) \in I \}.$$

We shall show that $1 \in J$ by pointing out two coprime elements of $K[X]$ in J. The elements $(X-\xi)^2$, $(\sqrt{F} - \lambda X - \nu)^2$ and $\sqrt{F} + \lambda X + \nu$ are in J. Consequently

$$\sqrt{F} \equiv -(\lambda X + \nu) \mod J$$

and

$$(\sqrt{F} - \lambda X - \nu)^2 - (\sqrt{F} + \lambda X + \nu)^2 = -4\sqrt{F}(\lambda X + \nu) \equiv F \equiv (\lambda X + \nu)^2 \equiv 0 \mod J,$$

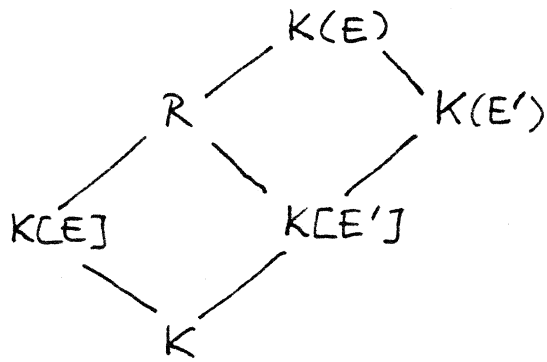
i.e. F and $(\lambda X + \nu)^2 \in J$. Suppose $X - \xi$ divides $\lambda X + \nu$. Since

$$(X-\xi)^2 \mid F - (\lambda X + \nu)^2 = \prod (X - x_i)$$

it would follow that $(X-\xi)^2 \mid F$ and since $\xi \in \{x_1, x_2\}$ either P or Q (or both) would be singular, a contradiction. Hence $(X-\xi)^2$ and $(\lambda X + \nu)^2$ are coprime elements of J. Hereby all cases are dealt with. $\square$.

§2. Norms and isogenies.

In this section we give a proof of theorem (I.4.6): a morphism induces a group homomorphism on the sets of points. Since this is clear for the trivial morphism we restrict ourselves to the case that $\varphi: E \to E'$ is an isogeny, with E, E' elliptic curves over a field K of characteristic $\neq 2,3$. We have to prove that $\varphi_L : E(L) \to E'(L)$ is a group homomorphism, for any field extension $L > K$. Since E and E' are elliptic curves over L, we need not talk about extensions and may assume $L = K$. If $\varphi = (f : g\sqrt{F} : 1)$ we have an embedding $\varphi^* : K(E') \hookrightarrow K(E)$ defined by $X' \mapsto f$, $\sqrt{F'} \mapsto g\sqrt{F}$. We identify the coordinate ring $K[E']$ with $K[f, g\sqrt{F}] \subset K(E)$, and put $R = K[X, \sqrt{F}, f, g\sqrt{F}]$. We have extensions of rings



Before proving that φ_K is a group homomorphism, we recall some linear algebra. Let L be a field of arbitrary characteristic, and V an n-dimensional vector space over L, for $n \geq 1$.

(2.1) Definition. A volume function on V is a map: $D: V^n \to L$ that satisfies:

(i) Multilinearity:

$$D(v_1, \cdots, \lambda v + \mu w, \cdots, v_n) = \lambda D(v_1, \cdots, v, \cdots, v_n) + \mu D(v_1, \cdots, w, \cdots, v_n)$$

(ii) Antisymmetry:

$D(v_1, \cdots, v_n) = 0$ if there exists $1 \leq i < n$ such that $v_i = v_{i+1}$.

See exercise (2.1) for elementary properties of volume functions. In particular it is shown there that if $\{e_1, \cdots, e_n\}$ is a basis of V, and $v = (v_1, \cdots, v_n) \in V^n$ with $v_i = \sum_j a_{ij} e_j$, then

$$Dv = \sum_{\sigma} \varepsilon(\sigma) \cdot a_{1,\sigma(1)} \cdot \ldots \cdot a_{n,\sigma(n)} \cdot D(e_1, \cdots, e_n),$$

where σ ranges over the permutations of $\{1, \cdots, n\}$ and $\varepsilon(\sigma)$ denotes the sign of σ.

(2.2) Proposition. The set of volume functions on V is a vector space of dimension 1 over L.

PROOF: It is clear that the volume functions form a vector space, with the evident scalar multiplication. By the remarks made above, a volume function D depends only on the value of $D(e_1, \cdots, e_n)$, which proves dimension ≤ 1, and it is straightforward to check that

$$Dv = \sum_{\sigma} \varepsilon(\sigma) \cdot a_{1,\sigma(1)} \cdot \cdots \cdot a_{n,\sigma(n)}$$

with notations as above, is multilinear and antisymmetric, which proves dimension ≥ 1. □

(2.3) Definition. Let T be a vectorspace of dimension $|V|^n$, with basis $\{e(v) \mid v \in V^n\}$. Let U be the subspace of T generated by

$$e(v_1, \cdots, \lambda v + \mu w, \cdots, v_n) - \lambda e(v_1, \cdots, v, \cdots, v_n) - \mu e(v_1, \cdots, w, \cdots v_n)$$

for $v, w, v_i \in V$ and $\lambda, \mu \in L$, and

$$e(v_1, \cdots, v_n) \text{ such that } \exists\, 1 \leq i < n : v_i = v_{i+1}.$$

for $v_i \in V$. We define the n-th external power $\Lambda^n V$ of V by

$$\Lambda^n V = T/U.$$

(2.4) Proposition. $\dim_L \Lambda^n V = 1$

PROOF: $\mathrm{Hom}_L(\Lambda^n V, L) \cong_L \{\text{volume functions on } V\}$. □

We denote the class of $e(v_1, \cdots, v_n)$ mod U in $\Lambda^n V$ by $v_1 \wedge \cdots \wedge v_n$. By the proposition $\Lambda^n V$ is generated by $e_1 \wedge \cdots \wedge e_n$, if $\{e_1, \cdots, e_n\}$ is a basis of V. The external power construction is functorial, i.e. an endomorphism $\varepsilon: V \to V$ induces a linear map $\Lambda^n \varepsilon : \Lambda^n V \to \Lambda^n V$ by $\Lambda^n \varepsilon (v_1 \wedge \cdots \wedge v_n) = \varepsilon v_1 \wedge \cdots \wedge \varepsilon v_n$.

(2.5) Definition. Let $\varepsilon : V \to V$ be an endomorphism. The determinant of ε, denoted $\det \varepsilon$, is the unique element of L such that $\Lambda^n \varepsilon = (\text{multiplication-by-} \det \varepsilon)$ on $\Lambda^n V$.

We now return to our isogeny $\varphi = (f : g\sqrt{F} : 1)$. Denote by I_E and $I_{E'}$ the groups of invertible ideals of $K[E]$ and $K[E']$ respectively. To show that φ_K is a group homomorphism, we shall define a map (norm):

$$N : I_E \to I_{E'}$$

such that

(i) N is a group homomorphism;

(ii) $NP_E \subset P_{E'}$;

(iii) The diagram

$$\begin{array}{ccc} I_E/P_E & \xrightarrow{\bar{N}} & I_{E'}/P_{E'} \\ \downarrow & & \downarrow \\ E(K) & \xrightarrow{\varphi_K} & E'(K) \end{array}$$

is commutative, the vertical arrows being the isomorphisms defined in the previous section.

The theorem readily follows from the existence of such a map. We use the following notation. Let $n = \deg \varphi$. Then $K(E)$ is an n-dimensional vector space over $K(E')$, with n^{th} external power $\Lambda^n K(E)$. For a finitely generated R-module $0 \neq H \subset K(E)$ we denote

$$\Lambda^n H = \text{subgroup of } \Lambda^n K(E) \text{ generated by } h_1 \wedge \cdots \wedge h_n,\ h_i \in H.$$

By exercise (2.3) $\Lambda^n H$ is a finitely generated $K[E']$-module $\neq 0$. By choosing an isomorphism $\Lambda^n K(E) \xrightarrow{\sim} K(E')$ we may identify all modules $\Lambda^n H$ with sub-$K[E']$-modules of $K(E')$. By exercise (1.2) the $\Lambda^n H$ thus become invertible $K[E']$ modules. Furthermore $\Lambda^n(\alpha H) = \det(\alpha) \cdot \Lambda^n H$ for $\alpha \in K(E)$, by definition of the determinant.

We now define the norm of an invertible $K[E]$-module M as the unique $K[E']$-module such that

$$\Lambda^n(R \cdot M) = N(M) \cdot \Lambda^n(R),$$

in other words

$$N(M) = \Lambda^n(RM) \cdot (\Lambda^n R)^{-1}.$$

(2.6) Lemma. $NP_E \subset P_{E'}$.

PROOF: $N(\alpha K[E]) = \Lambda^n(\alpha R) \cdot \Lambda^n(R)^{-1} = \det(\alpha) \cdot \Lambda^n R \cdot (\Lambda^n R)^{-1}$
$= \det(\alpha) \cdot K[E']$. □

(2.7) Lemma. N is a group homomorphism.

PROOF: Define the map

$$\chi : \Lambda^n K(E) \times \Lambda^n K(E) \to \Lambda^{2n}(K(E) \oplus K(E))$$

by

$$\chi(v_1 \wedge \cdots \wedge v_n, w_1 \wedge \cdots \wedge w_n) = (v_1, 0) \wedge \cdots \wedge (v_n, 0) \wedge (0, w_1) \wedge \cdots \wedge (0, w_n).$$

If H is an R-module, then

$$\chi(\Lambda^n H \times \Lambda^n H) = \Lambda^{2n}(H \oplus H),$$

and since χ is $K(E')$-linear

$$\chi(S\cdot\Lambda^n H \times \Lambda^n H) = \chi(\Lambda^n H \times S\cdot\Lambda^n H) = S\cdot\Lambda^{2n}(H\oplus H)$$

for any subset $S \subset K(E')$. In particular

$$\Lambda^{2n}(R\Pi \oplus R) = \chi(\Lambda^n R\Pi \times \Lambda^n R) = \chi(N(\Pi)\cdot\Lambda^n R \times \Lambda^n R)$$
$$= N(\Pi)\cdot\Lambda^{2n}(R\oplus R)$$

for $\Pi \in I_E$.

We have to show that $N(\Pi\Pi') = N(\Pi)\cdot N(\Pi')$ for $\Pi, \Pi' \in I_E$. We first deal with the case $\Pi + \Pi' = K[E]$. Let $\mu \in \Pi$ and $\mu' \in \Pi'$ be such that $\mu + \mu' = 1$, and let σ be the $K(E')$-automorphism of $K(E)\oplus K(E)$ defined by

$$\sigma(x,y) = (\mu' x - \mu y, x + y).$$

The inverse of σ is given by

$$\sigma^{-1}(a,b) = (a + \mu b, -a + \mu' b).$$

If $x \in R\Pi$ and $y \in R\Pi'$, then $\mu' x - \mu y \in R\Pi\Pi'$ and $x + y \in R\Pi + R\Pi' \subseteq R$. Conversely if $a \in R\Pi\Pi'$ and $b \in R$ the $a + \mu b \in R\Pi\Pi' + R\Pi \subseteq R\Pi$ and $-a + \mu' b \in R\Pi\Pi' + R\Pi' \subseteq R\Pi'$. Summarizing

$$\sigma(R\Pi \oplus R\Pi') = R\Pi\Pi' \oplus R.$$

It follows that

$$N(\Pi)\cdot N(\Pi')\cdot\Lambda^{2n}(R\oplus R) = \Lambda^{2n}(R\Pi \oplus R\Pi') = \det(\sigma^{-1})\cdot\Lambda^{2n}(R\Pi\Pi'\oplus R)$$
$$= \det(\sigma^{-1})\cdot N(\Pi\Pi')\cdot\Lambda^{2n}(R\oplus R) =$$
$$= N(\Pi\Pi')\cdot\Lambda^{2n}(\sigma(R\oplus R))$$
$$= N(\Pi\Pi')\cdot\Lambda^{2n}(R\oplus R).$$

Identifying $\Lambda^{2n}(R\oplus R)$ with an invertible $K[E']$-module this shows $N(\Pi)\cdot N(\Pi') = N(\Pi\Pi')$. To deal with the general case, we claim that for every $\Pi, \Pi' \in I_E$ there exist $\alpha, \alpha' \in K(E)^*$ such that $\alpha\Pi + \alpha'\Pi' = K[E]$. It then follows that

$$N(\Pi)\cdot N(\Pi') = \det(\alpha)^{-1}\cdot\det(\alpha')^{-1}\cdot N(\alpha\Pi)\cdot N(\alpha'\Pi')$$
$$= \det(\alpha^{-1})\cdot\det(\alpha'^{-1})\cdot N(\alpha\alpha'\Pi\Pi') = N(\Pi\Pi').$$

We leave the proof of the claim as an exercise (2.4). □

(2.8) <u>Lemma.</u> The diagram

$$\begin{array}{ccc} Cl_E & \xrightarrow{\bar{N}} & Cl_{E'} \\ \| & & \| \\ E(K) & \xrightarrow{\varphi_K} & E'(K) \end{array}$$

is commutative.

PROOF: By theorem(1.9) every invertible $K[E]$-module is equivalent to a module M_P for $P \in E(K)$, where

$$M_P = \begin{cases} K[E] & \text{if } P = \mathcal{O}; \\ K[X](X-x) + K[X](\sqrt{F}-y) & \text{if } P = (x:y:1). \end{cases}$$

To prove the lemma we have to show that $N(M_P) \sim M'_{\varphi(P)}$, the invertible $K[E']$-module belonging to $\varphi(P)$. In fact we shall show that equality holds. If $P = \mathcal{O}$ then this is clear.

If $P = (x:y:1)$ and $\varphi(P) = \mathcal{O}$ then $f_2(x) = 0$. (f_1 and f_2 are used to denote the numerator and and denominator of f in lowest terms as usual.) Hence $f_2 \in K[X]\cdot(X-x) \subseteq M_P$ and $f_1 = f_2 \cdot f \in M_P \cdot R$. Hence f_1 and f_2 are coprime elements of $K[X] \cap M_P \cdot R$, which shows that $M_P \cdot R = R$, and

$$N(M_P) = \Lambda^n(R) \cdot \Lambda^n(R)^{-1} = K[E'] = M'_{\mathcal{O}}$$

as required.

Now suppose that $P = (x:y:1)$ is not in the kernel of φ_K. Then $\varphi(P) = (f(x) : g(x)y : 1)$ and $M'_{\varphi(P)} = K[X'](X' - f(x)) + K[X'](\sqrt{F'} - g(x)y)$, with $X' = f$ and $\sqrt{F'} = g\sqrt{F}$.

We first show that $N(K[E](X-x)) = K[E'](X' - f(x))$. In section §4 of the notes we have seen that the minimum polynomial of X over $K(E')$ is $f_1(T) - X' f_2(T) \in K(E')[T]$. Hence the minimum polynomial of $X-x$ over $K(E')$ is

$$h = f_1(T+x) - X' f_2(T+x) = T^n + \sum_{i=0}^{n-1} a_i T^i .$$

The matrix of „multiplication-by-$(X-x)$" over the basis $\{1, X-x, \dots, (X-x)^{n-1}\}$ of $K(E)/K(E')$ is

$$\begin{pmatrix} 0 & 0 & \cdots & 0 & -a_0 \\ 1 & 0 & & \vdots & -a_1 \\ 0 & 1 & & \vdots & \vdots \\ \vdots & & \ddots & 0 & \\ 0 & \cdots & & 1 & -a_{n-1} \end{pmatrix} .$$

Hence

$$\begin{aligned} \det(X-x) &= (-1)^{n-1}(-a_0) = \pm h(0) \\ &= \pm\{ f_1(x) - X' f_2(x) \} \\ &= (\mp f_2(x) \in K^*) \cdot \{ X' - f(x) \}, \end{aligned}$$

so $N(K[E](X-x)) = K[E'](X' - f(x))$.

As we have seen in the proof of (1.9), $M_P \cdot M_{-P} = K[E](X-x)$ and $M'_{\varphi(P)} \cdot M'_{-\varphi(P)} = (X' - f(x))$. Since it is also clear that $-\varphi(P) = \varphi(-P)$, we see

$$N(M_P) \cdot N(M_{-P}) = N(K[E](X-x)) = K[E'](X' - f(x)) = M'_{\varphi(P)} \cdot M'_{\varphi(-P)} .$$

From $M_P \subset K[E]$ it follows that $N(M_P) \subset N(K[E]) = K[E']$ is an ideal.

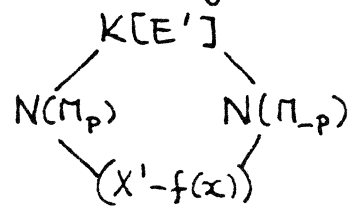
In exercise(2.5) it is shown that the ideals I with

$$K[E]\cdot(X'-f(x)) \subset I \subset K[E']$$

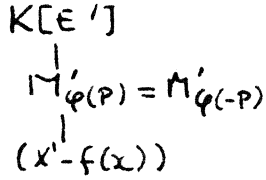
are in one to one correspondence with the divisors of the polynomial

$$(T-g(x)y)(T+g(x)y) \in K[T],$$

as illustrated in the diagram.

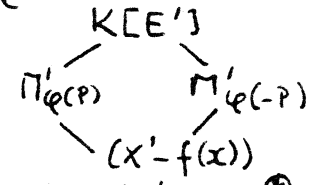


If $g(x)y = 0$ we have



so $N(\Pi_P)$ is one of these three ideals, and since $N(\Pi_P)^2 = (X'-f(x))$ we must have $N(\Pi_P) = M'_{\varphi(P)}$.

If $g(x)y \neq 0$ we have



and $N(\Pi_P) = M'_{\varphi(\pm P)}$ ②. To prove that $N(\Pi_P) = \Pi'_{\varphi(P)}$ we show that $(\sqrt{F}'-g(x)y)^n \in N(M_P)$.

Let $\lambda, \mu \in K[X]$ be such that $\lambda f_1 + \mu f_2 = 1$. Then $\frac{1}{f_2} = \lambda f + \mu \in R$ and since g_2 has the same factors as f,

$$\frac{1}{g_2} \in K[X]\cdot\frac{1}{f_2} \subseteq K[X]\cdot R = R.$$

Furthermore $X-x \mid g_1 - g(x)g_2$, so $g_1 - g(x)g_2 \in \Pi_P$, and

$$g - g(x) = g_2^{-1}(g_1 - g(x)g_2) \in R\cdot\Pi_P.$$

Since $\sqrt{F}-y \in \Pi_P$ we have

$$\sqrt{F}\cdot(g-g(x)) + g(x)\cdot(\sqrt{F}-y) = g\sqrt{F} - g(x)y = \sqrt{F}'-g(x)y \in R\cdot\Pi_P.$$

and

$$(\sqrt{F}'-g(x)y)^n = \det(\sqrt{F}'-g(x)y) \in \{s \in K(E') \mid s\cdot\Lambda^n R \subseteq \Lambda^n R\cdot\Pi_P\} = N(M_P). \square$$

---

② Let $\tau \in \mathrm{Aut}\,K(E)$ begiven by $\alpha+\beta\sqrt{F} \longmapsto \alpha-\beta\sqrt{F}$, and put $\tau' = \tau|_{K(E')}$. Then $\tau\Pi_P = \tau M_{-P}$ and by exercise(2.6)

$$\tau' N\Pi_P = N(\tau\Pi_P) = NM_{-P}.$$

Suppose $N\Pi_P = K[E']$ then $K[E'] = K[E']\cdot\tau' K[E'] = N\Pi_P\cdot\tau' N\Pi_P = N\Pi_P\cdot N\Pi_{-P} = (X'-f(x))$, a contradiction. Similarly $N\Pi_P \neq (X'-f(x))$.

§3. The dual isogeny.

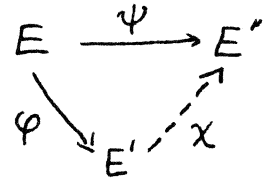
In exercise (9.5) of the notes we have mentioned a generalization of the notion of complex conjugation of endomorphisms. In this section we shall state and prove this result. In fact we shall prove a stronger theorem. As usual, K denotes a field of characteristic $\neq 2,3$.

(3.1) Theorem. Let E, E', E'' be elliptic curves over K, and $\varphi: E \to E'$ and $\psi: E \to E''$ isogenies such that

(i) $\ker \varphi_{\bar{K}} \subset \ker \psi_{\bar{K}}$;

(ii) $\deg_i \varphi \leq \deg_i \psi$.

Then there exists a unique morphism $\chi: E' \to E''$ such that $\chi \circ \varphi = \psi$.



We postpone the proof to the end of this section.

(3.2) Corollary. Let $\varphi \in \mathrm{Hom}_K(E, E')$ be a morphism. Then there exists a unique morphism $\hat{\varphi} \in \mathrm{Hom}_K(E', E)$ (the dual morphism), such that

(i) $\hat{\varphi} \circ \varphi = [\deg \varphi] \in \mathrm{End}_K(E)$;

(ii) $\varphi \circ \hat{\varphi} = [\deg \varphi] \in \mathrm{End}_K(E')$;

(iii) $\hat{\hat{\varphi}} = \varphi$.

Proof: If $\varphi = 0$ we can take $\hat{\varphi} = 0$, so we may assume that $\varphi = (f : g\sqrt{F} : 1)$ is an isogeny. By theorem (I.4.14)

$$\#\ker \varphi_{\bar{K}} = \deg_s \varphi \mid \deg \varphi,$$

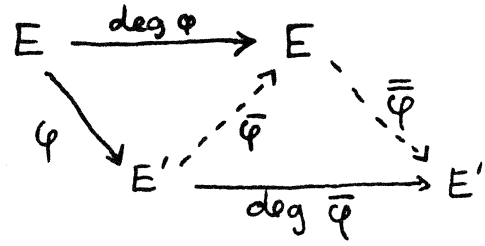
so if $P \in \ker \varphi_{\bar{K}}$ then $[\deg \varphi].P = 0$. This shows that $\ker \varphi_{\bar{K}} \subset \ker [\deg \varphi]_{\bar{K}}$. If $\mathrm{char}\, K = p > 0$ and $q = p^k$ and $p \nmid n$, then

$$\deg_i (qn) = \frac{\deg (qn)}{\deg_s (qn)} = \frac{q^2 n^2}{\#\ker (qn)_{\bar{K}}} = \frac{q^2 n^2}{q^i n^2} \geq q,$$

where $i \in \{0, 1\}$, cf. corollary (I.7.3). Hence if $\varphi = \varphi_{sep} \circ \mathrm{Frob}_q^m$ then $\deg \varphi = p^m \cdot q \cdot n$ with $p \nmid n$. (This includes the case $\mathrm{char}\, K = p = 0$: we put $0^0 = 1$.) We have

$$\deg_i \varphi = q \leqslant p^k \cdot q \leqslant \deg_i(\deg \varphi).$$

We can now apply the theorem with $\psi = [\deg \varphi]$.



There exists a unique $\bar{\varphi}$ that satisfies (i). Moreover

$$(\varphi \circ \bar{\varphi}) \circ \varphi = \varphi \circ (\bar{\varphi}\varphi) = \varphi \circ [\deg \varphi] = [\deg \varphi] \circ \varphi,$$

hence $\varphi\bar{\varphi} = [\deg \varphi]$ by exercise (4.5), and

$$\deg \varphi \cdot \deg \bar{\varphi} = \deg \varphi\bar{\varphi} = \deg(\deg \varphi) = (\deg \varphi)^2,$$

hence $\deg \varphi = \deg \bar{\varphi}$. By uniqueness it follows that $\bar{\bar{\varphi}} = \varphi$. □

Let $L \subset M$ be an arbitrary extension of fields. The group of <u>L-automorphisms</u> of M is defined as

$$\mathrm{Aut}_L(M) = \{ \sigma \in \mathrm{Aut}\, M \mid \sigma|_L = \mathrm{id}_L \}.$$

For any subgroup $G \subset \mathrm{Aut}\, M$ we denote

$$M^G = \{ x \in M \mid \forall \sigma \in G : \sigma(x) = x \}.$$

This is a subfield of M, called the field of <u>G-invariants</u>.

(3.3) <u>Proposition.</u> Suppose $M = L(\alpha)$ is a finite extension of L and G is a subgroup of $\mathrm{Aut}_L M$ such that $\#G = [M:L]$. Then

$$L = M^G$$

and

$$G = \mathrm{Aut}_L M.$$

PROOF: We have $L \subset M^G \subset M$. Let $f \in M^G[T]$ and $g \in L[T]$ be the minimum polynomials of α over M^G and L respectively. For every $\sigma \in \mathrm{Aut}_L M$ we have $g(\sigma(\alpha)) = \sigma(g(\alpha)) = 0$, hence $T - \sigma(\alpha) \mid g$ in $M[T]$. Similarly $T - \sigma(\alpha) \mid f$ for $\sigma \in G$. One easily verifies that $\sigma(\alpha) = \tau(\alpha)$ if and only if $\sigma = \tau$, for $\sigma, \tau \in \mathrm{Aut}_L M$. It follows that

$$\#G = \deg \prod_{\sigma \in G} (T - \sigma(\alpha)) \leqslant \deg f = [M:M^G] \leqslant [M:L] = \#G,$$

hence the inequalities are equalities, in particular $[M:M^G] = [M:L]$

and $M^G = L$. Also

$$\#\mathrm{Aut}_L M \leq \deg g = [M:L] = \#G,$$

whence $G = \mathrm{Aut}_L M$. □

We call a finite field extension $L \subset M$ a <u>finite Galois extensio</u> if it satisfies the hypotheses of the proposition, i.e. if $M = L(\alpha)$ and $\#\mathrm{Aut}_L M = [M:L]$. In this case $\mathrm{Aut}_L M$ is called the <u>Galois group</u> of $L \subset M$, and is usually denoted by $\mathrm{Gal}(M/L)$.

(3.4) Lemma. Let L, L' be field extensions of K, and σ a K-homomorphism $L \to L'$. If E is an elliptic curve over K, then σ induces a map $\sigma = \sigma_E : E(L) \to E(L')$, given by $\sigma(x:y:z) = (\sigma x : \sigma y : \sigma z)$. Further more, if $\varphi : E \to E'$ is a morphism then we have a commutative diagram

$$\begin{array}{ccc} E(L) & \xrightarrow{\sigma_E} & E(L') \\ \downarrow{\scriptstyle \varphi_L} & & \downarrow{\scriptstyle \varphi_{L'}} \\ E'(L) & \xrightarrow{\sigma_{E'}} & E'(L') \end{array}.$$

PROOF: Exercise. □

(3.5) <u>Proposition</u>. Let $\varphi : E \to E'$ be an isogeny, such that $\#\ker \varphi_K = \deg \varphi$. Then $K(E)/K(E')$ is finite Galois with group $\mathrm{Gal}(K(E)/K(E')) \cong \ker \varphi_K$.

PROOF: We define a map $E(K) \longrightarrow \mathrm{Aut}_K K(E)$ as follows. Consider the set of points $E(K(E))$ with generic point $P_0 = (X : \sqrt{F} : 1)$. For every $P \in E(K)$ we shall define an automorphism σ_P of $K(E)$, by specifying its values $\sigma_P(X)$ and

$\sigma_P(\sqrt{F})$. These are given by

$$(\sigma_P(X) : \sigma_P(\sqrt{F}) : 1) = P_0 + P \in E(K(E)).$$

First of all σ_P is a well defined map $K[E] \to K(E)$ since $\sigma_P((\sqrt{F})^2) = \sigma_P(F(X))$, and σ_P is a ring homomorphism by definition (we put $\sigma(x)=x$ for $x \in K$.). Secondly σ_P is injective since $\sigma_{-P} \circ \sigma_P(\alpha) = \alpha$ whenever $\alpha, \sigma_P(\alpha) \in K[E]$. Hence we can extend σ_P to $K(E)$, and it becomes a K-automorphism of $K(E)$, with inverse σ_{-P}. As

$$\sigma_{P+Q}(P_0) = P_0 + P + Q = \sigma_P P_0 + Q = \sigma_P P_0 + \sigma_P Q = \sigma_P \circ \sigma_Q(P_0),$$

the map $P \mapsto \sigma_P$ is a group homomorphism. (Note that $\sigma_P Q = Q$ since Q is rational.) If $\sigma_P = \sigma_Q$ then $P_0 + P = P_0 + Q$ and so $P = Q$. This shows that the defined map is an embedding

$$E(K) \hookrightarrow \mathrm{Aut}_K K(E).$$

Let $\varphi^* : K(E') \hookrightarrow K(E)$ be the embedding of the function fields, with $K(E') = K(X', \sqrt{F'})$. Now

$$\varphi^*(X' : \sqrt{F'} : 1) = (\varphi^* X' : \varphi^* \sqrt{F'} : 1) = (f(X) : g(X)\sqrt{F} : 1)$$
$$= \varphi_{K(E)}(X : \sqrt{F} : 1),$$

so if $P \in \ker \varphi_K$ then

$$\sigma_P(\varphi^* X' : \varphi^* \sqrt{F'} : 1) = \sigma_P \circ \varphi_{K(E)}(P_0)$$
$$= \varphi_{K(E)} \circ \sigma_P(P_0) \quad \text{(by lemma (3.4), with } L = L' = K(E)\text{)}$$
$$= \varphi_{K(E)}(P_0 + P)$$
$$= \varphi_{K(E)} P_0 + \varphi_{K(E)} P$$
$$= \varphi_{K(E)} P_0$$
$$= (\varphi^* X' : \varphi^* \sqrt{F'} : 1).$$

This shows that $\sigma_P | \varphi^* K(E') = \mathrm{id}$. Hence $\ker \varphi_K$ is mapped isomorphically to a subgroup of $\mathrm{Aut}_{K(E')} K(E)$. The proposition now follows from (3.3), together with the observation that $K(E) = K(E')(X)$ and $\#\ker \varphi_K = [K(E) : K(E')]$. □

In the proof of (3.1) we need yet another lemma.

(3.6) Lemma. Let $K \subset L$ be an extension of fields and

$f \in L(X)$. Suppose there exists $g = g_1/g_2 \in K(X)$ with $\deg g_1 > \deg g_2$, such that $f(g) \in K(X)$. Then $f \in K(X)$.

PROOF: For $h = h_1/h_2$ with $h_1, h_2 \in K[X]$ we put

$$lc(h) =_{def} \frac{\text{leading coefficient of } h_1}{\text{leading coefficient of } h_2}.$$

This does not depend of the representation of h. We first prove that $lc(f) \in K^*$ (assuming $f \neq 0$). If $f = f_1/f_2$ and $f_1 = a_0 + \cdots + a_n X^n$ then

$$f_1(g) = \frac{a_0 g_2^n + \cdots + a_n g_1^n}{g_2^n}.$$

Since $\deg g_1 > \deg g_2$ we have $lc(a_0 g_2^n + \cdots + a_n g_1^n) = a_n \cdot lc(g_1^n)$. Hence $lc\, f_1(g) = lc\, f_1 \cdot lc(g)^n$ and

$$lc\, f(g) = lc\, f \cdot (lc\, g)^{\deg f_1} \cdot (lc\, g)^{-\deg f_2}.$$

This is well defined since $g \neq 0$, and it shows that $lc\, f \in K^*$. We now show that $f \in K(X)$ by induction on $\deg f_1 + \deg f_2$, with $f = f_1/f_2$ reduced in lowest terms. By taking the inverse if necessary we may assume $k = \deg f_1 - \deg f_2 > 0$. Let

$$h = f - (lc\, f)^{-1} \cdot X^k = \frac{f_1 - (lc\, f)^{-1} X^k f_2}{f_2}.$$

Numerator and denominator of the latter expression are coprime, and $(lc\, f)^{-1} X^k f_2$ has the same leading coefficient and degree as f_1. Hence $\deg h_1 + \deg h_2 < \deg f_1 + \deg f_2$, and also $h(g) = f(g) - (lc\, f)^{-1} g^k \in K(X)$. By induction $h \in K(X)$ and $f = h + lc(f)^{-1} \cdot X^k \in K(X)$. □

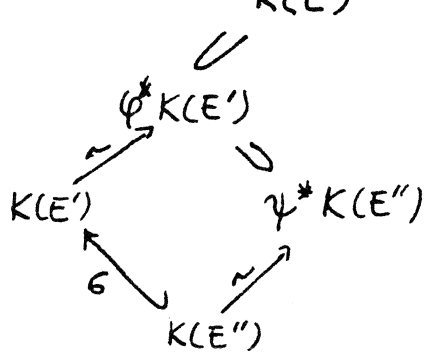
PROOF OF (3.1): If χ exists it is certainly unique by exercise( ). We prove existence in three steps of increasing generality.

Case 1: $\#\ker \varphi_K = \deg \varphi$ and $\#\ker \psi_K = \deg \psi$.

In this case φ and ψ are separable and $\ker \varphi_K = \ker \varphi_{\bar{K}} \subset \ker \psi_{\bar{K}} = \ker \varphi_K$, by theorem (4.14). We have two subfields $\varphi^* K(E')$ and $\psi^* K(E'')$ of $K(E)$, and applying proposition (3.5)

$$\psi^* K(E'') = K(E)^{\ker \psi_K} \subset K(E)^{\ker \varphi_K} = \varphi^* K(E').$$

This implies the existence of a homomorphism $\sigma : K(E'') \to K(E')$.



We shall show that σ is induced by an isogeny $\chi : E' \to E''$. We set $\varphi = (p : q\sqrt{F} : 1)$, $\psi = (r : s\sqrt{F} : 1)$ and $K(E') = K(X', \sqrt{F'})$, $K(E'') = K(X'', \sqrt{F''})$. Suppose $\sigma(X'') = t + v\sqrt{F'}$ with $t, v \in K(X')$. Then

$$r(X) = \psi^*(X'') = \varphi^* \circ \sigma(X'')$$
$$= t(p(X)) + v(p(X))\, q(X)\sqrt{F}.$$

Hence $v(p) \cdot q = 0$ and since $q \neq 0$ it follows that $v = 0$, and $\sigma(X'') = t \in K(X')$. In a similar manner we prove that $\sigma(\sqrt{F''}) = u\sqrt{F'} \in K(X') \cdot \sqrt{F'}$ and $u(p) \cdot q = s$. We claim that $\chi = (t : u\sqrt{F'} : 1)$ is an isogeny $E' \to E''$. If this is so then clearly $\chi^* = \sigma$ and $\chi\varphi = (t(p) : u(p) q \sqrt{F} : 1) = \psi$. First of all $\chi \in E''(K(E'))$ since

$$(u\sqrt{F'})^2 = \sigma(\sqrt{F''})^2 = \sigma(X''^3 + a'' X'' + b'')$$
$$= t^3 + a'' t + b''.$$

It remains to be shown that $\deg t_1 > \deg t_2$. Let $i_0 : K(E) \to K((T))$ be the well known embedding, and $d = \deg_T \circ i_0$ the induced valuation $K(E) \to \mathbb{Z} \cup \{\infty\}$. We have $t(p) = r$, and since i_0 is K-linear we can write this as

$$i_0 r \cdot t_2(i_0 p) = i_0 r \cdot i_0 t_2(p) = i_0 t_1(p) = t_1(i_0 p),$$

hence

$$dr + (\deg t_2) \cdot dp = (\deg t_1) \cdot dp.$$

However $dr, dp < 0$ since φ and ψ are isogenies, so

$$(\deg t_1 - \deg t_2) \cdot dp = dr < 0$$

and $\deg t_1 > \deg t_2$. This proves case 1.

Case 2: φ and ψ are separable.

By theorem (4.14) this reduces to case 1 for the algebraic

closure of K. We obtain an isogeny χ defined over $\bar{K}$, i.e. $t, u \in \bar{K}(X')$ (notations being as above). Now $t(p) = r \in K(X)$ and $u(p) = q/s \in K(X)$. Since $\deg p_1 > \deg p_2$ we can apply lemma (3.6) and find that χ is defined over K, which concludes case 2.

Case 3: φ and ψ arbitrary.

Say $\deg_i \varphi = p^A \leq p^B = \deg_i \psi$, where $\operatorname{char} K = p$. (Of course $0^0 = 1$.) We have factorizations

$$\varphi = \varphi_{sep} \circ \mathrm{Frob}_{p^A}$$

and

$$\psi = \psi_{sep} \circ \mathrm{Frob}_{p^B}.$$

The isogeny $\lambda = \mathrm{Frob}_{p^{B-A}} \circ \varphi_{sep}$ has inseparable degree p^{B-A} and factors as $\lambda = \lambda_{sep} \circ \mathrm{Frob}_{p^{B-A}}$. We obtain a commutative diagram

$$\begin{array}{ccccccc} E & \xrightarrow{\mathrm{Frob}_{p^A}} & E^{(p^A)} & \xrightarrow{\mathrm{Frob}_{p^{B-A}}} & E^{(p^B)} & \xrightarrow{\psi_{sep}} & E'' \\ & & \downarrow{\scriptstyle \varphi_{sep}} & & \downarrow{\scriptstyle \lambda_{sep}} & \nearrow{\scriptstyle \chi_{sep}} & \\ & & E' & \xrightarrow{\mathrm{Frob}_{p^{B-A}}} & E'^{(p^{B-A})} & & \end{array}$$

The existence of χ_{sep} follows from case 2, and $\chi = \chi_{sep} \circ \mathrm{Frob}_{p^B}$ is the required isogeny. This proves the general case and concludes the proof. □

Exercises.

1.1. Let F be a monic polynomial of odd degree in $K[X]$, and A an order in $K[X,\sqrt{F}]$. Let M be an invertible A-module.
(a) Show that $A = \{\alpha \in K(X,\sqrt{F}) \mid \alpha M \subset M\}$.
(b) Suppose M is an invertible A'-module. Show that $A' = A$.

1.2. Let F be a monic polynomial of odd degree in $K[X]$, and suppose $0 \neq M \subset K(X,\sqrt{F})$ is a finitely generated $K[X,\sqrt{F}]$-module.
(a) Show that $A = \{\alpha \in K(X,\sqrt{F}) \mid \alpha M \subset M\}$ is an order, and M is an invertible A-module.
(b) Suppose F is squarefree. Show that M is an invertible $K[X,\sqrt{F}]$-module.

1.3. Let F be a monic polynomial of degree 3 in $K[X]$. Show that $K[X,\sqrt{F}]$ is a principal ideal domain if and only if $F(x)$ is <u>not</u> a square in K for all $x \in K$.

1.4. Let $s,t \in \overline{K}$ with $s \neq t$ be such that $(X-s)^2(X-t) \in K[X]$. Show that $s,t \in K$.

<u>Remark:</u> in the four exercises above K is a field of characteristic $\neq 2$.

2.1 Let V be an n-dimensional vector space over L with basis $\{e_1,\cdots,e_n\}$, and let D be a volume function on V. Show that:
(a) $D(v_1,\cdots,v_n)=0$ if $\exists\, i \neq j$ with $v_i = v_j$, and $D(v_1,\cdots,v_i,\cdots,v_j,\cdots v_n) = -D(v_1,\cdots,v_j,\cdots,v_i,\cdots,v_n)$;
(b) if $v=(v_1,\cdots,v_n)$ with $v_i = \sum_j a_{ij} e_j$ then
$D(v) = \sum_{\sigma \in S_n} a_{1,\sigma(1)} \cdot \ldots \cdot a_{n,\sigma(n)} D(e_{\sigma(1)},\cdots,e_{\sigma(n)}) = \sum_{\sigma \in S_n} \varepsilon(\sigma) \cdot a_{1,\sigma(1)} \cdot \ldots \cdot a_{n,\sigma(n)} \cdot D(e_1,\cdots,e_n)$;
(c) if $v^t = (v_1^t,\cdots,v_n^t)$ with $v_i^t = \sum_j a_{ji} e_j$ then $D(v) = D(v^t)$.

2.2 Let V, L be as above. Choose for $v \in \Lambda^n V$ a matrix $A_v = (a_{ij})$ such that $v = \sum_j a_{1j} e_j \wedge \cdots \wedge \sum_j a_{nj} e_j$. Show that $\det A_v$ does not depend on the representation $v = v_1 \wedge \cdots \wedge v_n$, but does depend on the choice of basis. Show that $v \mapsto \det A_v$ is an isomorphism $\Lambda^n V \longrightarrow L$.

2.3. Let $R = K[X,\sqrt{F},X',\sqrt{F'}]$ be as in §2, and let $0 \neq H \subset K(E)$ be a finitely generated R-module.
(a) Show that R is a finitely generated $K[E']$-module with generators $\{1,X,\cdots,X^{n-1},\sqrt{F},X\sqrt{F},\cdots,X^{n-1}\sqrt{F}\}$. Conclude that H is finitely generated $K[E']$-module
(b) Show that H generates $K(E)$ over $K(E')$ and $H \cap K[E'] \neq 0$. [Hint: $1 \in H \cdot K(E')$.]
(c) Show that $\Lambda^n H$ is a finitely generated $K[E']$-module, and $\Lambda^n H \neq 0$.

2.4. Let for $P=(x:y:1) \in E(K)$ be given $M_P = K[X](X-x) + K[X](\sqrt{F}-y) \in I_E$. Show that:
(a) $M_P + M_Q = K[E]$ if $P \neq Q$;
(b) $M_P \sim M_{-P} \cdot M_{2P}$ and $M_P + M_{-P} \cdot M_{2P} = K[E]$ if $P \neq -P$;
(c) $M_P \sim K[X]G + K[X]\sqrt{F}$ and $M_P + K[X]G + K[X]\sqrt{F} = K[E]$ if $P = -P$, where $G = F/(X-x) \in K[X]$. [Hint: $M_P(K[X]G + K[X]\sqrt{F}) = K[X,\sqrt{F}] \cdot (\sqrt{F})$]
(d) Finish the proof of proposition (2.7).

2.5. Let $(x:y:1) \in E(K)$. Show that $K[E]/(X-x) \cong K[T]/((T-y)(T+y))$, where T is a transcendental variable.

2.6. Let $\tau \in \mathrm{Aut}\, K(E)$ be given by $\alpha+\beta\sqrt{F} \mapsto \alpha-\beta\sqrt{F}$ and $\tau' \in \mathrm{Aut}\, K(E')$ by $\alpha+\beta\sqrt{F'} \mapsto \alpha-\beta\sqrt{F'}$, where $\alpha,\beta \in K(x)$ (resp. $K(x')$). Let $H \subset K(E)$ be an invertible R-module.

(a) Let $h = h_1 \wedge \cdots \wedge h_n \in \Lambda^n H$ be represented by $A_h = (a_{ij}) \in \mathrm{Mat}_n(K(E'))$, where $h_i = \sum_{d=1}^{\infty} a_{ij} x^{i-1}$. Show that $\tau h_1 \wedge \cdots \wedge \tau h_n \mapsto \tau'(\det A_h)$ under the isomorphism $\Lambda^n K(E) \xrightarrow{\sim} K(E')$ as defined in exercise (2.2)

(b) Let M be an invertible $K[E]$-module. Show that τM is an invertible $K[E]$-module, and $N(\tau M) = \tau'(NM)$.

3.1. Let E be an elliptic curve over K and $\varphi \in \mathrm{End}_K(E)$. Show that the dual $\bar{\varphi}$ as defined in (3.2) is equal to the complex conjugate of φ as defined in §9 of the notes.

Extra exercises to §4 of the notes.

4.5. Let $\psi : E \to E'$ and $\chi, \chi' : E' \to E''$ be isogenies such that $\chi\psi = \chi'\psi$. Show that $\chi = \chi'$.

4.6. Let $\varphi : E \to E'$ and $\psi : E' \to E''$ be morphisms. Show that $\deg(\psi \circ \varphi) = \deg(\psi) \cdot \deg(\varphi)$. [Hint: reduce to the separable case.]

2.7. Let $\{e_1, \ldots, e_n\}$ and $\{e_1', \ldots, e_n'\}$ be bases of $K(E)$ over $K(E')$, and define α by $\alpha(e_i) = e_i'$. Let $\varphi, \varphi' : \Lambda^n K(E) \to K(E')$ be given by $\varphi(e_1 \wedge \cdots \wedge e_n) = 1$ and $\varphi'(e_1' \wedge \cdots \wedge e_n') = 1$ respectively.

(a) Let $H \subset K(E)$ be a finitely generate R-module. Show that $\varphi(\Lambda^n H) = \det(\alpha) \cdot \varphi'(\Lambda^n H)$.

(b) Show that the norm of an invertible $K[E]$-module does not depend on a particular choice of isomorphism $\Lambda^n K(E) \xrightarrow{\sim} K(E')$.