Theorem statements from Chapter 2 of Washington

GROUP LAW. *Let E be an elliptic curve defined by $y^2 = x^3 + Ax + B$. Let $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ be points on E with $P_1, P_2 \neq \infty$. Define $P_1 + P_2 = P_3 = (x_3, y_3)$ as follows:*

1. *If $x_1 \neq x_2$ then*
$$x_3 = m^2 - x_1 - x_2, \qquad y_3 = m(x_1 - x_3) - y_1, \qquad \text{where } m = \frac{y_2 - y_1}{x_2 - x_1}.$$
2. *If $x_1 = x_2$ but $y_1 \neq y_2$, the $P_1 + P_2 = \infty$.*
3. *If $P_1 = P_2$ and $y_1 \neq 0$, then*
$$x_3 = m^2 - 2x_1, \qquad y_3 = m(x_1 - x_3) - y_1, \qquad \text{where } m = \frac{3x_1^2 + A}{2y_1}.$$
4. *If $P_1 = P_2$ and $y_1 = 0$, then $P_1 + P_2 = \infty$.*

Moreover, define
$$P + \infty = P$$
for all points P on E.

THEOREM 2.1. *The addition of points on an elliptic curve E satisfies the following properties:*

1. *(commutativity) $P_1 + P_2 = P_2 + P_1$ for all P_1, P_2 on E.*
2. *(existence of identity) $P + \infty = P$ for all points P on E.*
3. *(existence of inverse) Given P on E, there exists P' on E with $P + P' = \infty$. This point P' will usually be denoted $-P$.*
4. *(associativity) $(P_1 + P_2) + P_3 = P_1 + (P_2 + P_3)$ for all P_1, P_2, P_3 on E.*

In other words, the points on E form an additive abelian group with ∞ as the identity element.

INTEGER TIMES A POINT. *Let k be a positive integer and let P be a points on an elliptic curve. The following procedure computes kP.*

1. *Start with $a = k, B = \infty, C = P$.*
2. *If a is even, let $a = a/2$, and let $B = B, C = 2C$.*
3. *If a is odd, let $a = a - 1$, and let $B = B + C, C = C$.*

4. If $a \neq 0$, go to step 2.

5. Output B.

The output B is kP (see Exercise 2.8).

LEMMA 2.2. *Let $G(u,v)$ be a nonzero homogeneous polynomial and let $(u_0 : v_0) \in \mathbf{P}^1_k$. Then there exists an integer $k \geq 0$ and a polynomial $H(u,v)$ with $H(u_0, v_0) \neq 0$ such that*

$$G(u,v) = (v_0 u - u_0 v)^k H(u,v).$$

LEMMA 2.3. *Let L_1 and L_2 be lines intersecting in a point P, and, for $i = 1, 2$, let $L_i(x,y,z)$ be a linear polynomial defining L_i. Then $\mathrm{ord}_{L_1,P}(L_2) = 1$ unless $L_1(x,y,z) = \alpha L_2(x,y,z)$ for some constant α, in which case $\mathrm{ord}_{L_1,P}(L_2) = \infty$.*

DEFINITION 2.4. *A curve C in $\mathbf{P}^2_K$ defined by $F(x,y,z) = 0$ is said to be* **nonsingular** *at a point P if at least one of partial derivatives F_x, F_y, F_z is nonzero at P.*

LEMMA 2.5. *Let $F(x,y,z) = 0$ define a curve C. If P is a nonsingular point of C, then there is exactly one line in $\mathbf{P}^2_K$ that intersects C to order at least 2, and it is the tangent to C at P.*

THEOREM 2.6. *Let $C(x,y,z)$ be a homogeneous cubic polynomial, and let C be the curve in $\mathbf{P}^2_K$ described by $C(x,y,z) = 0$. Let ℓ_1, ℓ_2, ℓ_3 and m_1, m_2, m_3 be lines in $\mathbf{P}^2_K$ such that $\ell_i \neq m_j$ for all i, j. Let P_{ij} be the point of intersection of ℓ_i and m_j. Suppose P_{ij} is a nonsingular point on the curve C for all $(i,j) \neq (3,3)$. In addition, we require that if, for some i, there are $k \geq 2$ of the points P_{i1}, P_{i2}, P_{i3} equal to the same point, then ℓ_i intersects C to order at least k at this point. Also, if, for some j, there are $k \geq 2$ of the points P_{1j}, P_{2j}, P_{3j} equal to the same point, then m_j intersects C to order at least k at this point. Then P_{33} also lies on the curve C.*

LEMMA 2.7. *Let $R(u,v)$ and $S(u,v)$ be homogeneous polynomials of degree 3, with $S(u,v)$ not identically 0, and suppose there are three points $(u_i : v_i)$, $i = 1,2,3$, at which R and S vanish. Moreover, if k of these points are qual to the same point, we require that R and S vanish to order at least k at this point (that is, $(v_i u - u_i v)^k$ divides R and S). Then there is a constant $\alpha \in K$ such that $R = \alpha S$.*

LEMMA 2.8. *$D(x,y,z)$ is a multiple of $\ell_1(x,y,z) m_1(x,y,z)$.*

LEMMA 2.9. *$\ell(P_{22}) = \ell(P_{23}) = \ell(P_{32}) = 0$*

LEMMA 2.11. *Let P_1, P_2 be points on an elliptic curve. Then $(P_1 + P_2) - P_2 = P_1$ and $-(P_1 + P_2) + P_2 = -P_1$*

THEOREM 2.13 (Pascal's Theorem)**.** *Let $ABCDEF$ be a hexagon inscribed in a conic section (ellipse, parabola, or hyperbola), where A, B, C, D, E, F are distinct points in the affine plane. Let X be the intersection of $\overline{AB}$ and $\overline{DE}$, let Y be the intersection of $\overline{BC}$ and $\overline{EF}$, and let Z be the intersection of $\overline{CD}$ and $\overline{FA}$. Then X, Y, Z are collinear (see Figure 2.4).*

COROLLARY 2.15 (Pappus's Theorem)**.** *Let ℓ and m be two distinct lines in the plane. Let A, B, C be distinct points of ℓ and let A', B', C' be distinct points of m. Assume that none of these points is the intersection of ℓ and m. Let X be the intersection of $\overline{AB'}$ and $\overline{A'B}$, let Y be the intersection of $\overline{B'C}$ and $\overline{BC'}$, and let Z be the intersection of $\overline{CA'}$ and $\overline{C'A}$. Then X, Y, Z are collinear (see Figure 2.5).*

PROPOSITION 2.16. *Let K be a field of characteristic not 2 and let*

$$y^2 = x^3 + ax^2 + bx + c = (x - e_1)(x - e_2)(x - e_3)$$

be an elliptic curve E over K with $e_1, e_2, e_3 \in K$. Let

$$x_1 = (e_2 - e_1)^{-1}(x - e_1), \qquad y_1 = (e_2 - e_1)^{-3/2} y, \qquad \lambda = \frac{e_3 - e_1}{e_2 - e_1}.$$

Then $\lambda \neq 0, 1$ and

$$y_1^2 = x_1(x_1 - 1)(x_1 - \lambda)$$

THEOREM 2.17. *Let K be a field of characteristic not 2. Consider the equation*

$$v^2 = au^4 + bu^3 + cu^2 + du + q^2$$

with $a, b, c, d, q \in K$. Let

$$x = \frac{2q(v + q) + du}{u^2}, \qquad y = \frac{4q^2(v + q) + 2q(du + cu^2) - (d^2u^2/2q)}{u^3}.$$

Define

$$a_1 = d/q, \qquad a_2 = c - (d^2/4q^2), \qquad a_3 = 2qb$$

$$a_4 = -4q^2 a, \qquad a_6 = a_2 a_4. \quad (1)$$

Then

$$y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6.$$

The inverse transformation is

$$u = \frac{2q(x + c) - (d^2/2q)}{y}, \qquad v = -q + \frac{u(ux - d)}{2q}.$$

The point $(u, v) = (0, q)$ corresponds to the point $(x, y) = \infty$ and $(u, v) = (0, -q)$ corresponds to $(x, y) = (-a_2, a_1 a_2 - a_3)$.

PROPOSITION 2.18. *Let K be a field of characteristic not 2. Let $c, d \in K$ with $c, d \neq 0$ and d not a square in K. The curve*

$$C : u^2 + v^2 = c^2(1 + du^2v^2)$$

is isomorphic to the elliptic curve

$$E : y^2 = (x - c^4 d - 1)(x^2 - 4c^4 d)$$

via the change of variables

$$x = \frac{-2c(w - c)}{u^2}$$

$$y = \frac{4c^2(w - c) + 2c(c^4 d + 1)u^2}{u^3}$$

where $w = (c^2du^2 - 1)v$. The point $(0, c)$ is the identity for the group law on C and the addition law is

$$(u_1, v_1) + (u_2, v_2) = \left(\frac{u_1 v_2 + u_2 v_1}{c(1 + du_1u_2v_1v_2)}, \frac{v_1 v_2 - u_1 u_2}{c(1 - du_1u_2v_1v_2)} \right)$$

for all points $(u_i, v_i) \in C(K)$. The negative of a point is $-(u, v) = (-u, v)$.

THEOREM 2.19. *Let $y_1^2 = x_1^3 + A_1x_1 + B_1$ and $y_2^2 = x_3^2 + A_2x_2 + B_2$ be two elliptic curves with j-invariants j_1 and j_2, respectively. If $j_1 = j_2$, then there exists $\mu \neq 0$ in $\overline{K}$ (= algebraic closure of K) such that*

$$A_2 = \mu^4 A_1, \qquad B_2 = \mu^6 B_1.$$

The transformation

$$x_2 = \mu^2 x_1, \qquad y_2 = \mu^3 y_1$$

takes one equation to the other.

LEMMA 2.20. *Let E be defined over $\mathbf{F}_q$. Then ϕ_q is an endomorphism on E of degree q, and ϕ_q is not separable.*

PROPOSITION 2.21. *Let $\alpha \neq 0$ be a separable endomorphism of an elliptic curve E. Then*

$$\deg \alpha = \#\mathrm{Ker}(\alpha),$$

where $\mathrm{Ker}(\alpha)$ is the kernel of the homomorphism $\alpha : E(\overline{K}) \to E(\overline{K})$.

If $\alpha \neq 0$ is not separable, then

$$\deg \alpha > \#\mathrm{Ker}(\alpha).$$

THEOREM 2.22. *Let E be an elliptic curve defined over a field K. Let $\alpha \neq 0$ be an endomorphism of E. Then $\alpha : E(\overline{K}) \to E(\overline{K})$ is surjective.*

LEMMA 2.24. *Let E be the elliptic curve $y^2 = x^3 + Ax + B$. Fix a point (u, v) on E. Write*

$$(x, y) + (u, v) = (f(x, y), g(x, y)),$$

where $f(x, y)$ and $g(x, y)$ are rational functions of x, y (the coefficients depend on (u, v)) and y is regarded as a function of x satisfying $dy/dx = (3x^2 + A)/(2y)$. Then

$$\frac{\frac{d}{dx} f(x, y)}{g(x, y)} = \frac{1}{y}.$$

LEMMA 2.26. *Let $\alpha_1, \alpha_2, \alpha_3$ be nonzero endomorphisms of an elliptic curve E with $\alpha_1 + \alpha_2 = \alpha_3$. Write*

$$\alpha_j(x, y) = (R_{\alpha_j}(x), yS_{\alpha_j}(x)).$$

Suppose there are constants $c_{\alpha_1}, c_{\alpha_2}$ such that

$$\frac{R'_{\alpha_1}(x)}{S_{\alpha_1}(x)} = c_{\alpha_1}, \qquad \frac{R'_{\alpha_2}(x)}{S_{\alpha_2}(x)} = c_{\alpha_2}.$$

Then

$$\frac{R'_{\alpha_3}(x)}{S_{\alpha_3}(x)} = c_{\alpha_1} + c_{\alpha_2}.$$

PROPOSITION 2.28. *Let E be an elliptic curve defined over a field K, and let n be a nonzero integer. Suppose that multiplication by n on E is given by*

$$n(x, y) = (R_n(x), yS_n(x))$$

for all $(x, y) \in E(\overline{K})$, where R_n and S_n are rational functions. Then

$$\frac{R_n'(x)}{S_n(x)} = n.$$

Therefore, multiplication by n is separable if and only if n is not a multiple of the characteristic p of the field.

PROPOSITION 2.29. *Let E be an elliptic curve defined over $\mathbf{F}_q$, where q is a power of the prime p. Let r and s be integers, both not 0. The endomorphism $r\phi_q + s$ is separable if and only if $p \nmid s$.*