Section 1. The Group Law on an Elliptic Curve

Lemma. Let $P_1, \ldots, P_8$ be such that no 4 points lie on a line and no 7 points lie on a conic. Then there exists a unique point P_9 which is a 9th point of intersection of any two cubics passing through $P_1, \ldots, P_8$. *(Proof Optional).*

(1) Theorem. Let $\mathcal{C}$ be an elliptic curve $/K$, with K-rational point $\underline{\mathbf{o}}$. Then $\mathbf{a} + \mathbf{b}$, as in Definition 1.2, gives a commutative group law on the points on $\mathcal{C}$, with identity $\underline{\mathbf{o}}$. The inverse of $\mathbf{a}$ is given by the point $-\mathbf{a}$, constructed in in Definition 1.2. Further, the K-rational points $\mathcal{C}(K)$ form a subgroup, called the *Mordell-Weil group.*

Theorem (Hasse). Let $\mathcal{E}$ be an elliptic curve over $\mathbb{F}_p$. Let $N_p = \#\mathcal{E}(\mathbb{F}_p)$ where, as usual, $\mathcal{E}(\mathbb{F}_p)$ should be taken to including $\underline{\mathbf{o}}$ [so that N_p is the number of affine points (x, y) on $\mathcal{E}$ with $x, y \in \mathbb{F}_p$, plus 1, to include the point at infinity $\underline{\mathbf{o}}$]. Then:

$$|N_p - (p+1)| \leqslant 2\sqrt{p}, \text{ that is, } N_p \in [(p+1) - 2\sqrt{p}, (p+1) + 2\sqrt{p}].$$

Similarly, any curve $y^2 = Q(x)$, where $Q(x) = f_4x^4 + \ldots + f_0$ has nonzero discriminant, has at least $p - 1 - 2\sqrt{p}$ affine points. *(Proof Optional).*

Section 2. The p-adic Numbers $\mathbb{Q}_p$

(2) Lemma. The function $|\ |_p$ is a non-Archimedean valuation on $\mathbb{Q}$.

(3) Theorem. Let K be a field, complete with respect to a non-Archimedean valuation $|\ |$, and let x_n be a sequence in K. Then: $x_n \to 0$ in $K \iff \sum x_n$ is convergent in K.

(4) Theorem (Hensel's Lemma). Let K be a field, complete with respect to a non-Archimedean valuation $|\ |$, with valuation ring $R = \{x \in K : |x| \leqslant 1\}$.

Let $f(x) \in R[x]$ and let $a_0 \in R$ satisfy: $\quad |f(a_0)| < |f'(a_0)|^2. \qquad (*)$

Then there exists a unique $a \in R$ such that $f(a) = 0$ and $|a - a_0| \leqslant |f(a_0)|/|f'(a_0)|$.

(5) Corollary. Let $\alpha \in \mathbb{Q}_p$ with $|\alpha|_p = 1$. When $p \neq 2$, α is a square in $\mathbb{Q}_p$ iff it is a square modulo p. When $p = 2$, α is a square in $\mathbb{Q}_p$ iff $\alpha \equiv 1 \pmod 8$.

Section 3. The Reduction Map on an Elliptic Curve

(6) Theorem. Let $\mathcal{C}$ be defined over K, written so that the coefficients lie in R. Let $\widetilde{\mathcal{C}}$, defined over k, be the reduction of $\mathcal{C}$ modulo $\mathcal{M}$. Let $b \in \widetilde{\mathcal{C}}(k)$ be a nonsingular point. Then b lifts to $\mathcal{C}$; that is, there exists $a \in \mathcal{C}(K)$ such that $\tilde{a} = b$.

(7) Theorem. Let $\mathcal{C} : F(X_0, X_1, X_2) = 0$ be a cubic curve defined over K, written so that coefficients of F have maximum valuation 1. Suppose the line $\mathcal{L} : L(X_0, X_1, X_2) = 0$ meets $\mathcal{C}$ at a, b, c. Then either:

(1) $\widetilde{\mathcal{L}} \subset \widetilde{\mathcal{C}}$, that is, $\widetilde{F}(X_0, X_1, X_2) = \widetilde{L}\widetilde{M}$, for some M.

or:

(2) $\widetilde{\mathcal{L}}$ meets $\widetilde{\mathcal{C}}$ precisely at $\tilde{a}, \tilde{b}, \tilde{c}$.

(8) Lemma. Any point (x, y) on $\mathcal{E}$ [$\leftrightarrow$ (z, w) on $\mathcal{E}'$] in the kernel of reduction [namely: $|x| > 1, |y| > 1 \leftrightarrow |z| < 1, |w| < 1$] is uniquely determined by z, with $w = w(z) \in \mathbb{Z}[A, B][[z]]$. The group law is completely described by the above $F_{\mathcal{E}}(z_1, z_2) \in \mathbb{Z}[A, B][[z_1, z_2]]$, which converges to the z-coordinate of the sum of $(z_1, w(z_1))$ and $(z_2, w(z_2))$.

Section 4. Formal Groups

(9) Lemma. Let $F(X, Y)$ be a formal group over a ring R, and let R_T denote $R[[T]]$.

(1) There is a unique power series $i(T) \in TR_T$ such that $F\big(T, i(T)\big) = 0$.

(2) $F(X, 0) = X$ and $F(0, Y) = Y$.

(10) Lemma. Let $a \in R^*$ [that is: $a \in R$ and $a^{-1} \in R$], and let $f(T) \in TR_T$ be of the form $f(T) = aT + \ldots$ Then there exists a unique $g(T) \in TR_T$ such that $f(g(T)) = T$. Furthermore, g satisfies $g(f(T)) = T$.

(11) Lemma. The homomorphism $[m] : F \to F$ is an isomorphism whenever $m \in R^*$.

(12) Theorem. Let F be a formal group over R. There exists a unique normalised invariant differential given by $\omega(T) = F_X(0, T)^{-1}\mathrm{d}T \in R_T\mathrm{d}T$. Every invariant differential is of the form $a\omega$ for some $a \in R$.

(13) Corollary. Let f be a homomorphism over R from the formal group F to the formal group G. Let ω_F, ω_G be the normalised invariant differentials on F, G, respectively. Then $\omega_G \circ f = f'(0)\ \omega_F$.

(14) Corollary. Let F be a formal group over R and let, as usual, $[m](T) \in R_T$ denote the multiplication by m map on F. Let p be prime. Then there exist $f, g \in R_T$ [$f(T) = T + \ldots$], such that $[p](T) = pf(T) + g(T^p)$.

(15) Theorem. Let R be a field of characteristic 0; then $\log_F$ [as in the previous definition] is an isomorphism from F to $\widehat{G}_a$, the additive group $X + Y$.

(16) Lemma. Let $F, K, R, \mathcal{M}, k$ [with $\mathrm{char}(k) = p$] be as in Definition 4.17.

(a) The identity map: $F(\mathcal{M}^n)/F(\mathcal{M}^{n+1}), \oplus \to \mathcal{M}^n/\mathcal{M}^{n+1}, +$ is an isomorphism.

(b) Every torsion element of $F(\mathcal{M})$ has order a power of p.

(17) Theorem. Let $F, K, R, \mathcal{M}, k$ [with $\mathrm{char}(k) = p$] be as in Defn 4.17. Suppose that $z \in F(\mathcal{M})$ has exact order p^n, for some $n \geqslant 1$, so that $[p^n](z) = 0$, but $[p^{n-1}](z) \neq 0$. Then:

$$|z| \geqslant |p|^{\frac{1}{p^n - p^{n-1}}}.$$

(18) Corollary. Let $\mathcal{E} : y^2 = x^3 + Ax + B$, be an elliptic curve, where $A, B \in \mathbb{Z}_p$. The kernel $\mathcal{E}_1(\mathbb{Q}_p)$ of the reduction map $\sim : \mathcal{E}_0(\mathbb{Q}_p) \to \widetilde{\mathcal{E}}_{ns}(\mathbb{F}_p)$ has no torsion (apart from $\underline{\mathbf{o}}$). Any $(x, y) \in \mathcal{E}_{\text{tors}}(\mathbb{Q}_p)$ satisfies $|x|_p \leqslant 1, |y|_p \leqslant 1$. When $\widetilde{\mathcal{E}}$ is non-singular, $\mathcal{E}_{\text{tors}}(\mathbb{Q}_p)$ is isomorphic to a subgroup of $\widetilde{\mathcal{E}}(\mathbb{F}_p)$.

Section 5. Global Torsion

(19) Lemma. Let $\mathcal{E} : y^2 = x^3 + Ax + B$, where $A, B \in \mathbb{Z}$, be an elliptic curve [so that $\Delta = 4A^3 + 27B^2 \neq 0$]. Let p be a prime satisfying: $p \neq 2$ and $p \not| \ \Delta$ (such a prime is said to be of *good reduction*, since $\widetilde{\mathcal{E}}$ mod p is still an elliptic curve over $\mathbb{F}_p$). Then $\mathcal{E}_{\text{tors}}(\mathbb{Q})$ is isomorphic to a subgroup of $\widetilde{\mathcal{E}}(\mathbb{F}_p)$, and so $\#\mathcal{E}_{\text{tors}}(\mathbb{Q}) \mid \#\widetilde{\mathcal{E}}(\mathbb{F}_p)$.

(20) Lemma. Let $(x_1, y_1) \neq \underline{\mathbf{o}}$ be a $\mathbb{Q}$-rational torsion point on $\mathcal{E} : y^2 = x^3 + Ax + B$, where $A, B \in \mathbb{Z}$. Then $x_1, y_1 \in \mathbb{Z}$.

(21) Theorem (Nagell-Lutz). Let $\underline{\mathbf{o}} \neq (x_1, y_1) \in \mathcal{E}_{\text{tors}}(\mathbb{Q})$, where $\mathcal{E} : y^2 = x^3 + Ax + B$, and $A, B \in \mathbb{Z}$. Then $x_1, y_1 \in \mathbb{Z}$ and either $y_1 = 0$ or $y_1^2 \mid \Delta$, where $\Delta = 4A^3 + 27B^2$.

Section 6. A 2-isogeny on an Elliptic Curve

(22) Lemma. Let $\mathcal{C} : Y^2 = X(X^2 + aX + b)$, where $a, b \in \mathbb{Z}, b \neq 0, a^2 - 4b \neq 0$, and let $\mathcal{D} : V^2 = U(U^2 + a_1U + b_1)$, where $a_1 = -2a$ and $b_1 = a^2 - 4b$.

$$\text{Define } \ \phi : \mathcal{C} \longrightarrow \mathcal{D} \ \text{ by } \ \phi(x, y) = \Big(\Big(\frac{y}{x}\Big)^2, y - \frac{by}{x^2}\Big).$$

$$\text{Define } \ \hat{\phi} : \mathcal{D} \longrightarrow \mathcal{C} \ \text{ by } \ \hat{\phi}(u, v) = \Big(\frac{1}{4}\Big(\frac{v}{u}\Big)^2, \frac{1}{8}\Big(v - \frac{b_1 v}{u^2}\Big)\Big).$$

Then the 2-isogenies $\phi, \hat{\phi}$ are 2-to-1 homomorphisms, each with kernel $\{\underline{\mathbf{o}}, (0, 0)\}$. Since $\phi, \hat{\phi}$ are defined over $\mathbb{Q}$, we also have $\phi : \mathcal{C}(\mathbb{Q}) \to \mathcal{D}(\mathbb{Q})$ and $\hat{\phi} : \mathcal{D}(\mathbb{Q}) \to \mathcal{C}(\mathbb{Q})$. The compositions $\hat{\phi} \circ \phi$ and $\phi \circ \hat{\phi}$ are the multiplication by 2 maps [2] on $\mathcal{C}$ and $\mathcal{D}$, respectively.

(23) Lemma. Let $\mathcal{C}, \mathcal{D}, \phi$ be as in Lemma 6.1, and let (u, v) be a point on $\mathcal{D}$ with $u \neq 0$. Let

$$x_1 = \big(u + u^{-1/2}v - a\big)/2, \quad y_1 = u^{1/2}x_1 = u^{1/2}\big(u + u^{-1/2}v - a\big)/2,$$
$$x_2 = \big(u - u^{-1/2}v - a\big)/2, \quad y_2 = -u^{1/2}x_1 = -u^{1/2}\big(u - u^{-1/2}v - a\big)/2.$$

Then $\phi(x_1, y_1) = \phi(x_2, y_2) = (u, v)$.

(24) Lemma. Let $(u, v) \in \mathcal{H}$. Then:

$$(u, v) \in \phi(\mathcal{G}) \iff u \in (\mathbb{Q}^*)^2 \text{ or } [u = 0 \text{ and } a^2 - 4b \in (\mathbb{Q}^*)^2].$$

(25) Lemma. The map $q : \mathcal{H} \to \mathbb{Q}^*/(\mathbb{Q}^*)^2$ of Definition 6.4 is a homomorphism with kernel $\phi(\mathcal{G})$ (so that the induced map $q : \mathcal{H}/\phi(\mathcal{G}) \to \mathbb{Q}^*/(\mathbb{Q}^*)^2$ is an injective homomorphism).

(26) Lemma. The map $q : \mathcal{H} \to \mathbb{Q}^*/(\mathbb{Q}^*)^2$ of Definition 6.4 has finite image. Indeed, if $r \in \mathbb{Q}^*/(\mathbb{Q}^*)^2$ is written as a square free integer, then $r \in \text{im } q \implies r|b_1$. Under q, $\mathcal{H}/\phi(\mathcal{G})$ is isomorphic to the subgroup of $\mathbb{Q}^*/(\mathbb{Q}^*)^2$ consisting of all square free integers $r|b_1$ such that

$$W_r : r\ell^4 + a_1\ell^2m^2 + (b_1/r)m^4 = n^2, \quad \text{for some } \ell, m, n \in \mathbb{Z}, \text{not all 0, with } \gcd(\ell, m) = 1.$$

When this is satisfied, there is a point $(u, v) \in \mathcal{H}$ such that $q(u, v) = r$, satisfying $u = r\big(\frac{\ell}{m}\big)^2$.

(27) Comment. If we similarly define $\hat{q} : \mathcal{G} \to \mathbb{Q}^*/(\mathbb{Q}^*)^2$ by:

$$\hat{q}(x, y) = \begin{cases} x & \text{when } x \neq 0 \\ b = a_1^2 - 4b_1 & \text{when } x = 0, \end{cases}$$

and $\hat{q}(\underline{\mathbf{o}}) = 1$, then, by the same argument, $\hat{q}$ has finite image. If $r \in \mathbb{Q}^*/(\mathbb{Q}^*)^2$ is written as a square free integer, then $r \in \text{im } \hat{q} \implies r|b$. Under $\hat{q}$, $\mathcal{G}/\hat{\phi}(\mathcal{H})$ is isomorphic to the subgroup of $\mathbb{Q}^*/(\mathbb{Q}^*)^2$ consisting of all square free integers $r|b$ such that

$$\widehat{W_r} : r\ell^4 + a\ell^2m^2 + (b/r)m^4 = n^2, \quad \text{for some } \ell, m, n \in \mathbb{Z}, \text{not all 0, with } \gcd(\ell, m) = 1.$$

When $\widehat{W_r}$ is satisfied, there is a point $(x, y) \in \mathcal{G}$ such that $q(x, y) = r$, satisfying $x = r\big(\frac{\ell}{m}\big)^2$.

(28) Theorem. Both $\mathcal{G}/\hat{\phi}(\mathcal{H})$ and $\mathcal{H}/\phi(\mathcal{G})$ are finite.

(29) Corollary. (The Weak Mordell-Weil Theorem, for an elliptic curve $\mathcal{C}$ which has a rational point of order 2). $\mathcal{G}/2\mathcal{G} = \mathcal{C}(\mathbb{Q})/2\mathcal{C}(\mathbb{Q})$ is finite.

Section 7. The Mordell-Weil Theorem

Lemma. Let $\mathcal{E}$ be an elliptic curve, defined over $\mathbb{Q}$. Define $h_x : \mathcal{E}(\mathbb{Q}) \to \mathbb{R}$ by:

$$h_x\big((x, y)\big) = \log \max\big(|a|, |b|\big), \quad \text{where } x = \frac{a}{b},\ a, b \in \mathbb{Z},\ \gcd(a, b) = 1,$$

and define $h_x(\underline{\mathbf{o}}) = 0$. Then h_x is a height function on $\mathcal{E}(\mathbb{Q})$. Indeed, there exists a constant C, independent of P, Q, such that $|h_x(P + Q) + h_x(P - Q) - 2h_x(P) - 2h_x(Q)| \leq C$, for all $P, Q \in \mathcal{E}(\mathbb{Q})$, from which properties (1),(2) can be deduced [property (3) is trivially true]. *(Proof Optional).*

(30) Theorem. Let A be an Abelian group which has a height function h, and suppose that $A/2A$ is finite. Then A is finitely generated.

(31) Theorem (The Mordell-Weil Theorem). Let $\mathcal{E}$ be any elliptic curve over $\mathbb{Q}$. Then $\mathcal{E}(\mathbb{Q})$ is finitely generated.