

1 Projective Planes

- given k a field, the affine n -space \mathbb{A}^n is constructed
- by identifying "projective" points (can be considered at "infinity") with directions in \mathbb{A}^n , the projective n -space \mathbb{P}^n is constructed
- this gives the relation $\mathbb{P}^n = \mathbb{A}^n \cup \mathbb{P}^{n-1}$

2 Weierstraß Equations

- Weierstraß equation: in simplest form, takes the form: $y^2 = ax^3 + bx + c$ (assuming $\text{char}(k) \neq 2, 3$)
- defines a curve over \mathbb{A}^2 , which can be extended to via homogenization ($Y^2Z = aX^3 + bXZ^2 + cZ^3$) and then to \mathbb{P}^2 by imposing $Z = 0$
- results in elliptic curve over \mathbb{P}^2 with one point at infinity, allowing for Bézout to hold

3 Bézout's Theorem

- let C_1 and C_2 be projective curves with no common components
- then, $\sum_{P \in C_1 \cap C_2} I(C_1 \cap C_2, P) = (\deg C_1)(\deg C_2)$, where I denotes intersection multiplicity

4 Group Structure on Curves

- two classes of curves: singular (cusps) and non-singular (smooth)
- singular curves permit easy parameterizations (and thus groups with trivial structures)
- non-singular curves admit obscure group structures

5 Group Law on Non-Singular Elliptic Curves

- define an additive abelian group with \mathcal{O} as the point at infinity
- given two points, $P, Q \in E(k)$:
 - take the line connecting P and Q and find its other intersection with $E(k)$, call it $-(P + Q)$
 - take the line connecting $-(P + Q)$ and \mathcal{O} ; the resulting intersection is $(P + Q)$
- easy to verify identity, inverses and commutativity

6 Group Law Formulae

- easily derivable through some algebra
- given $P = (x_1, y_1)$ $Q = (x_2, y_2)$, take λ to be the slope of the line joining P, Q
- this results in $P + Q = (x_3, y_3)$, where $x_3 = (\lambda^2 - a - x_1 - x_2)$, $y_3 = -\lambda x_3 - (y_1 - \lambda x_1)$

7 Heights of Points

- given $x = (m, n) \in E(\mathbb{Q})$ $\gcd(m, n) = 1$, we define the (naïve) height of x to be $H(x) = \max(|m|, |n|)$, and the corresponding logarithmic height to be $h(x) = \log H(x)$
- this induces a height on curves $E(\mathbb{Q})$, for if $E(\mathbb{Q}) \ni P = (x, y)$, then $h(P) = h(x)$ (we ignore y)
- this is almost a bi-linear form — in particular:
 - for each $Q \in E(\mathbb{Q})$ we have κ_0 , $h(P + Q) \leq 2 \cdot h(P) + \kappa_0 \forall P \in E(\mathbb{Q})$
 - there is κ , so that $h(2P) \geq 4 \cdot h(P) - \kappa$

8 Canonical Heights

- any naïve height induces the same canonical height
- define $\hat{h} = \lim_{n \rightarrow \infty} \frac{h(2^n P)}{4^n}$ — by Néron-Tate, we have:
 - $\hat{h}(P + Q) + \hat{h}(P - Q) = 2 \cdot \hat{h}(P) + 2 \cdot \hat{h}(Q)$
 - $\hat{h}(mP) = m^2 \cdot \hat{h}(P)$
 - $\langle P, Q \rangle = \hat{h}(P + Q) - \hat{h}(P) = \hat{h}(Q)$ is a bilinear form
 - $\hat{h}(P) = 0 \iff P \in E(\mathbb{Q})_{\text{tor}}$

9 Discrete Logarithms in $E(\mathbb{Q})$

- assuming $P = mQ$ for $P, Q \in E(\mathbb{Q})$ and some $m \in \mathbb{Z}$, m is easily found via the canonical height
- $m = \sqrt{\frac{\hat{h}(P)}{\hat{h}(Q)}}$