18.786: Topics in Algebraic Number Theory (spring 2006)
Supplement: addition on elliptic curves

Let K be a field and let $\overline{K}$ be an algebraic closure of K. Then any homogeneous polynomial $P \in K[x, y, z]$ defines a closed subvariety $V(P)$ of the projective space $\mathbb{P}^3_{\overline{K}}$. Actually it's a closed subscheme, but I'll often assume that P has no repeated factors, so that I can neglect this.

I say P is *nonsingular* at a point $[a : b : c] \in V(P)$ (the a, b, c being homogeneous coordinates) if the partial derivatives of P do not all vanish at $(x, y, z) = (a, b, c)$. Then P has a unique tangent line at that point.

For $P, Q \in K[x, y, z]$ homogeneous polynomials with no factors in common, I define the *intersection multiplicity* of P, Q at a point $[a : b : c] \in V(P) \cap V(Q)$ to be the K-dimension of the local ring of the scheme $V(P) \cap V(Q)$ at $[a, b, c]$. Concretely, take $K[x, y, z]/(P, Q)$, invert any homogeneous polynomial not vanishing at $[a, b, c]$, then pull out the bit of degree zero.

If P and Q are both nonsingular, then the intersection multiplicity is 1. If only P is nonsingular, then the intersection multiplicity is the order of vanishing of Q along the tangent line of P.

Theorem 1 (Bézout) *Let $P, Q \in K[x, y, z]$ be homogeneous polynomials with no repeated factors and no factors in common. Then the intersection multiplicities of all points of $V(P) \cap V(Q)$ add up to* $\deg(P) \deg(Q)$.

Let $P \in K[x, y, z]$ be a polynomial with no repeated factors. Let $\mathrm{Div}(P)$ be the free abelian group generated by $V(P)$; we refer to elements of $\mathrm{Div}(P)$ as *divisors* on P and define the *degree* of a divisor as the sum of its coefficients. For any $Q \in K[x, y, z]$ with no factor in common with P, write (Q) for the divisor consisting of each point in $V(P) \cap V(Q)$ with multiplicity equal to the intersection multiplicity. By Bézout, this divisor has degree $\deg(P) \deg(Q)$.

Let $\mathrm{Div}^0(P)$ be the subgroup of $\mathrm{Div}(P)$ consisting of divisors of degree 0. Define the *Picard group* $\mathrm{Pic}(P)$ of P (or better, of the algebraic curve $V(P)$ over $\overline{K}$) to be the quotient of $\mathrm{Div}^0(P)$ by the subgroup generated by $(Q_1) - (Q_2)$ for all homogeneous polynomials Q_1, Q_2 of the same degree.

Now suppose P has degree 3 and is nonsingular everywhere, and that $O \in V(P)$ is a point with coefficients in K. The pair $(V(P), O)$ is an example of an *elliptic curve*. In this case, for any points $T, U \in V(P)$, you can draw a line through T and U which hits $V(P)$ in a third point S, and thus get a relation $(S) + (T) + (U) = \ell$, where ℓ is the divisor of any fixed line. Consequence: every element of $\mathrm{Pic}(P)$ can be represented by a pair $(T) - (O)$ for some $T \in V(P)$. Moreover, this T is unique: that amounts to saying that $(T) - (U)$ can never occur as the divisor of a polynomial. That's a little exercise in the theory of algebraic curves: such a divisor would give rise to an isomorphism between $V(P)$ and $\mathbb{P}^1_{\overline{K}}$, but the former has genus 1 and the latter has genus 0. (Concretely: there is a rational differential form on $V(P)$ with no poles anywhere, but any rational differential on $\mathbb{P}^1_{\overline{K}}$ has two more poles than zeroes, when counting with multiplicity.)

In other words, there is an addition law for points on $V(P)$! Moreover, you can compute this law as follows: given two points T, U, take the third intersection S of the line through them with $V(P)$, then take the third intersection of the line through S and O with $V(P)$. In particular, K-rational points form a subgroup under addition.

Aside: the uniqueness argument doesn't work if P is degree 3 but singular, but you can still use the geometric addition law on nonsingular points, as long as O itself is nonsingular: you can prove the associativity by degeneration from the nonsingular case. (The hangup with a singular point is that a line through it always has intersection multiplicity greater than 1 with $V(P)$.) But in this case you can sometimes identify the result more simply; see exercises.

For more, see Silverman, *The Arithmetic of Elliptic Curves.* I may have more to say on this topic later.

Exercise (not to be turned in):

1. Let $P = x^3 + y^2 z$ and let $O = [0 : 1 : 0]$. Give an isomorphism of the group of nonsingular points of $V(P)$ with the *additive* group of $\overline{K}$.
2. Let $P = x^3 + x^2 z + y^2 z$ and let $O = [0 : 1 : 0]$. Give an isomorphism of the group of nonsingular points of $V(P)$ with the *multiplicative* group of $\overline{K}$.