

# Notes on Diophantine Geometry

Mohammad Moinul Haque

February 19, 2008

For the lecture given on 2/14/2008 by Felipe Voloch

## 1 Elliptic curves

**Definition:** If  $K$  is a field then an elliptic curve  $E$  over  $K$  is a smooth irreducible projective curve of genus 1 with a point  $P \in E(K)$

Question: Is it possible to decide if a curve of genus 1 over  $\mathbb{Q}$  has a point over  $\mathbb{Q}$ ?

*Answer:* There is a procedure which conjecturally works.

**Proposition:** Every elliptic curve over a field of characteristic  $\neq 2, 3$  is isomorphic to a curve of the type

$$y^2 = x^3 + ax + b$$

for some  $a, b \in K, 4a^3 + 27b^2 \neq 0$  with the given point  $P$  mapping to  $(0 : 1 : 0) = \mathcal{O}$ .

Group law on  $E$ :

$\mathcal{O}$  is the identity, and if  $P = (x, y)$  then  $-P = (x, -y)$ . By definition we have  $\forall P, P + (-P) = \mathcal{O}$  and  $P + \mathcal{O} = P$ .

Let  $P_1 = (x_1, y_1), P_2 = (x_2, y_2) \in E(K)$ . If  $x_1 \neq x_2$  then let

$$\alpha := \frac{y_1 - y_2}{x_1 - x_2}$$

otherwise (where  $P_1 = P_2$ )

$$\alpha := \frac{3x_1^2 + a}{2y_1}.$$

We then have  $P_1 + P_2 = (x_3, y_3)$  where

$$\begin{aligned} x_3 &:= \alpha^2 - x_1 - x_2 \\ y_3 &:= -(\alpha(x_3 - x_1) + y_1) \end{aligned}$$

Geometrically the point  $(x_3, -y_3)$  is the third point of intersection of the line passing through  $P_1$  and  $P_2$  with the elliptic curve. Substituting the equation of the line into the equation for  $E$ , we get

$$(\alpha(x - x_1) + y_1)^2 = x^3 + ax + b$$

which becomes

$$x^3 - \alpha^2 x^2 + \dots = 0$$

since  $x_1, x_2, x_3$  are the roots we get  $x_1 + x_2 + x_3 = \alpha^2$  and so forth.

Also,  $P + Q + R = \mathcal{O}$  iff  $P, Q, R$  are collinear.

One can prove associativity of the group law either by brute force computation or by using methods of classical geometry.

Two elliptic curves are isomorphic over an algebraically closed field if they have the same  $j$ -invariant. In other words,  $E$  is isomorphic to  $E'$  iff  $j(E) = j(E')$ , where

$$j(E) = \frac{1728a^3}{4a^3 + 27b^2},$$

so for example, changing  $x$  to  $\lambda^{-2}x$  and  $y$  to  $\lambda^{-3}y$  gives us  $y^2 = x^3 + \lambda^4 ax + \lambda^6 b$  which is isomorphic to our original curve.

If  $\Lambda \subseteq \mathbb{C}$  is a lattice, then  $\mathbb{C}/\Lambda \cong E(\mathbb{C})$  under  $z \mapsto (\wp(z), \wp'(z)/2)$ , where

$$\wp(z) = \frac{1}{z^2} + \sum_{\lambda \in \Lambda, \lambda \neq 0} \left( \frac{1}{(z + \lambda)^2} - \frac{1}{\lambda^2} \right).$$

**Definition:** An abelian variety is a smooth projective irreducible variety together with a (abelian) group law defined by rational functions in the coordinates.

(Elliptic curves are abelian varieties of dimension 1.)

### The Mordell-Weil Theorem:

**Theorem**(Mordell-Weil): If  $K$  is a global field and  $A/K$  is an abelian variety then  $A(K)$  is a finitely generated abelian group.

*Aside Question:* Is the group law unique? No, because in any abelian group, given  $g_0$  the map  $(g, h) \mapsto g + h - g_0$  is a group law with identity  $g_0$ . But, other than that, yes.

**Theorem:** If  $f : A \rightarrow A'$  is a regular map of abelian varieties with  $f(0) = 0$  then  $f$  is a group homomorphism.

*Aside Question:* Can conics have a group structure? Yes, for example consider  $xy = 1$  with  $(x_1, y_1)(x_2, y_2) = (x_1 x_2, y_1 y_2)$ . This only works for affine curves, not projective ones.

Aside Question: Are there other varieties with group laws, or non-abelian ones? Yes, known as group varieties. For example  $GL_n \subseteq \mathbb{A}^{n^2}$ , the set of  $n \times n$  matrices with nonzero determinant.

In general, the analogue Mordell-Weil does not hold. For example, if  $X$  denotes the affine conic  $xy = 1$  as above,  $X(\mathbb{Q}) = \mathbb{Q}^\times$  is not finitely generated.

Exercise: If  $y^2 = x^3 + x^2$  (a nodal cubic) then  $C_0(K) \cong K^\times$ , and if  $y^2 = x^3$  (a cuspidal cubic) then  $C_0(K) \cong (K, +)$ , where  $C_0 := C - \{(0, 0)\}$ . In other words, the same formulas define a group law for the given curves (with the groups mentioned) after we remove the singular point.

Remark: The first curve in the above exercise is an example of a semi-abelian variety. For those, the integer points form a finitely generated group. This generalizes both the Mordell-Weil Theorem and the Dirichlet Unit Theorem.

Strategy for the proof of the Mordell-Weil Theorem:

Here we assume  $K$  is a global field throughout.

*Step 1:* First prove the Weak Mordell-Weil Theorem, which states: If  $m \geq 2$  is an integer then  $A(K)/mA(K)$  is finite, where  $mA(K) := \{mP; P \in A(K)\}$ .

*Step 2:* Use height functions: There exist  $h : A(K) \rightarrow \mathbb{R}_{\geq 0}$  so that

- (a)  $\forall c > 0, \{P \in A(K); h(P) \leq c\}$  is finite
- (b)  $h(mP) = m^2h(P) + \mathcal{O}(1), P \in A(K)$
- (c)  $\forall P_0 \in A(K), \exists c \in (P_0)$  such that  $h(P + P_0) \leq 2h(P) + c(P_0)$ .

Remark: For an elliptic curve over  $\mathbb{Q}$ ,  $h(x, y) = \log(\max\{|p|, |q|\})$  where  $x = p/q$  with  $p, q \in \mathbb{Z}$  and  $(p, q) = 1$ .

We claim Step 1 and Step 2 imply the Mordell-Weil Theorem:

Let  $P_1, \dots, P_r$  be representatives for the classes of  $A(K)/mA(K)$ . Given  $Q \in A(K)$ ,  $\exists i \in \{1, \dots, r\}$  and  $R \in A(K)$  so that  $Q - P_i = mR$ , giving  $Q = mR + P_i$ . Let  $c = \max\{c(-P_1), \dots, c(-P_r)\}$  constants from property (c) of the height functions, then

$$h(Q - P_i) = h(mR) = m^2h(R) + c'$$

for some constant  $c'$  by property (b), and

$$m^2h(R) + c' \leq 2h(Q) + c$$

by property (c). Hence

$$h(R) \leq \frac{2}{m^2}h(Q) + \frac{c - c'}{m^2}$$

so letting  $c'' = (c - c')/m^2$  we have

$$\frac{2}{m^2}h(Q) + c'' \geq h(R)$$

so, choosing  $\lambda, 2/m^2 < \lambda < 1$ , either  $h(R) < \lambda h(Q)$  or

$$h(Q) \left( \lambda - \frac{2}{m^2} \right) \leq c''.$$

Therefore we have  $h(R) < \lambda h(Q)$  for some  $\lambda < 1$ , or  $h(Q) \leq c'''$  where  $c''' = c''/(\lambda - 2/m^2)$ . Note that the restriction  $h(Q) \leq c'''$  gives us a finite set.

Start with an arbitrary  $Q$  and put  $Q' = R$  and repeat until we have  $h(Q^{(k)}) \leq c'''$ , that is,

$$\begin{aligned} Q &= mQ' + P_i \\ Q' &= mQ'' + P_{i'} \\ &\vdots \\ Q^{(k)} & \end{aligned}$$

where  $h(Q^{(k)}) \leq c'''$  which will happen eventually since otherwise  $h(Q^{(i)}) \leq \lambda^i h(Q)$  which goes to 0 as  $i$  grows.

Since  $Q = mQ' + P_i = m(mQ'' + P_{i'}) + P_i = m^2Q'' + mP_{i'} + P_i, \dots$  we have

$$Q = m^k Q^{(k)} + \sum_{i=1}^r a_i P_i$$

therefore  $\{P_1, \dots, P_r\} \cup \{P; h(P) \leq c'''\}$ , a finite set, generate  $A(K)$ .